

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

50021537 VS
\$2

JCS31 U.S. PTO
09/741668



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
this Office.

願年月日
Date of Application:

1999年12月20日

願番号
Application Number:

平成11年特許願第361225号

願人
Applicant(s):

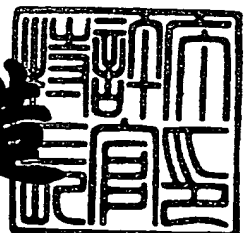
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月13日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 9900698611

【提出日】 平成11年12月20日

【あて先】 特許庁長官殿

【国際特許分類】 H09L 12/16

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 野中 聡

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 江崎 正

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

特平 1 1 - 3 6 1 2 2 5

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置、データ処理機器およびその方法

【特許請求の範囲】

【請求項 1】

コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置において、

第 1 のバスと、

前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第 1 のバスに接続された演算処理回路と、

前記第 1 のバスに接続された記憶回路と、

第 2 のバスと、

前記第 1 のバスと前記第 2 のバスとの間に介在するインターフェイス回路と、

前記第 2 のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、

前記第 2 のバスに接続された外部バスインターフェイス回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項 2】

前記インターフェイス回路を第 1 のインターフェイス回路とした場合に、前記第 1 のバスは、前記演算処理回路および前記記憶回路に接続された第 3 のバスと、前記第 1 のインターフェイス回路に接続された第 4 のバスとを有し、

前記データ処理装置は、

前記第 3 のバスと前記第 4 のバスとの間に介在する第 2 のインターフェイス回路

を前記耐タンパ性の回路モジュール内にさらに有する請求項 1 に記載のデータ処理装置。

【請求項 3】

第 5 のバスと、

記録媒体または IC カードに搭載された認証機能を持つデータ処理回路との間

の通信処理を行い、前記第 5 のバスに接続された第 3 のインターフェイス回路と

前記第 4 のバスと前記第 5 のバスとの間に介在する第 4 のインターフェイス回路と

を前記耐タンパ性の回路モジュール内にさらに有する請求項 2 に記載のデータ処理装置。

【請求項 4】

前記暗号処理回路は、

公開鍵暗号回路と、

共通鍵暗号回路と

を有する請求項 1 に記載のデータ処理装置。

【請求項 5】

前記記憶回路は、当該データ処理装置の秘密鍵データおよび他の装置の公開鍵データを記憶し、

前記公開鍵暗号回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する前記公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成し、

前記共通鍵暗号回路は、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する

請求項 4 に記載のデータ処理装置。

【請求項 6】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路

を前記耐タンパ性の回路モジュール内にさらに有し、

前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う

請求項 5 に記載のデータ処理装置。

【請求項 7】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成し、前記第 2 のバスに接続された乱数生成回路

を前記耐タンパ性の回路モジュール内にさらに有する

請求項 1 に記載のデータ処理装置。

【請求項 8】

前記外部バスインターフェイス回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路と接続される

請求項 1 に記載のデータ処理装置。

【請求項 9】

前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路と

をさらに有する請求項 8 に記載のデータ処理装置。

【請求項 10】

前記外部バスインターフェイス回路は、当該データ処理装置が搭載された機器の制御を統括的に行うホスト演算処理装置に接続される

請求項 1 に記載のデータ処理装置。

【請求項 11】

前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路をさらに有する請求項 8 に記載のデータ処理装置。

【請求項 12】

前記演算処理回路は、前記権利書データが示す取り扱いに基づいて、前記コン

テンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する

請求項 1 に記載のデータ処理装置。

【請求項 1 3】

前記演算処理回路は、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成し、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する

請求項 1 2 に記載のデータ処理装置。

【請求項 1 4】

前記共通鍵暗号回路は、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する

請求項 4 に記載のデータ処理装置。

【請求項 1 5】

有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、

前記記憶回路は、前記ライセンス鍵データを記憶し、

前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し

前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、

前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する

請求項 4 に記載のデータ処理装置。

【請求項 1 6】

前記記憶回路は、ブロック単位でデータの書き込みおよび消去が行われ、

前記演算処理回路によって制御され、前記記憶回路に対してのデータの書き込みおよび消去の許否を前記ブロック単位で管理する書き込みロック制御回路

を前記耐タンパ性の回路モジュール内にさらに有する請求項 1 に記載のデータ

処理装置。

【請求項 1 7】

コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置において、

第 1 のバスと、

前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第 1 のバスに接続された演算処理回路と、

前記第 1 のバスに接続された記憶回路と、

第 2 のバスと、

前記第 1 のバスと前記第 2 のバスとの間に介在するインターフェイス回路と、

前記第 2 のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、

前記第 2 のバスに接続された外部バスインターフェイス回路と

を耐タンパ性の回路モジュール内に有し、

前記演算処理回路は、前記外部バスインターフェイス回路を介して外部回路から割り込みを受けると、当該外部回路のスレーブとなって当該割り込みによって指定された処理を行い、当該処理の結果を前記外部装置に通知する

データ処理装置。

【請求項 1 8】

前記演算処理回路は、前記処理の結果を前記外部回路に割り込みを出して通知する

請求項 1 7 記載のデータ処理装置。

【請求項 1 9】

前記外部バスインターフェイスは、前記演算処理回路および前記外部回路との共有メモリを有し、

前記演算処理回路は、当該共有メモリに前記処理の結果を書き込み、当該処理の結果は前記外部回路からのポーリングによって当該外部回路に通知される

請求項 1 7 に記載のデータ処理装置。

【請求項 2 0】

前記外部バスインターフェイスは、

前記外部回路から依頼された処理の前記演算処理回路における実行状態を示し、前記演算処理回路によって設定され、前記外部回路によって読まれるフラグを持つ第 1 のステータスレジスタと、

前記外部回路が前記演算処理回路に処理を依頼したか否かを示し、前記外部回路によって設定され、前記演算処理回路によって読まれるフラグを持つ第 2 のステータスレジスタと、

前記処理の結果が書き込まれる記憶回路と

を有する請求項 1 9 に記載のデータ処理装置。

【請求項 2 1】

前記記憶回路は、前記割り込みによって指定される処理を記述した割り込みプログラムを記憶し、

前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行して前記処理を行う

請求項 1 8 に記載のデータ処理装置。

【請求項 2 2】

前記記憶回路は、複数の前記割り込みプログラムと、当該割り込みプログラムを実行する際に読み出される複数のサブルーチンとを記憶し、

前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行する際に、前記記憶回路から必要に応じて前記サブルーチンを読み出して実行する

請求項 2 1 に記載のデータ処理装置。

【請求項 2 3】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置と

を有するデータ処理機器において、

前記データ処理装置は、

権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段と

を耐タンパ性の回路モジュール内に有する

データ処理機器。

【請求項 2 4】

前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、

前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する

請求項 2 3 に記載のデータ処理機器。

【請求項 2 5】

前記データ処理装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する

請求項 2 3 に記載のデータ処理機器。

【請求項 2 6】

前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、

前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る

請求項 2 3 に記載のデータ処理機器。

【請求項 2 7】

前記データ処理装置は、

前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示し、前記演算処理装置によって読まれるフラグを持つ第 1 のステータスレジスタと

前記演算処理装置が当該データ処理装置に前記割り込みによって処理を依頼したか否かを示し、前記演算処理装置によって設定されるフラグを持つ第2のステータスレジスタと、

前記処理の結果が書き込まれる前記共有メモリと

を有する請求項26に記載のデータ処理機器。

【請求項28】

前記演算処理装置と、前記データ処理装置とを接続するバス

をさらに有する請求項23に記載のデータ処理機器。

【請求項29】

前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる

請求項24に記載のデータ処理機器。

【請求項30】

前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する

請求項24に記載のデータ処理機器。

【請求項31】

前記演算処理装置は、所定のユーザプログラムを実行する

請求項23に記載のデータ処理機器。

【請求項32】

データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理機器において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記デー

タ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第 1 の処理モジュールと、

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置であって、前記受信したモジュールに格納された権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納されたコンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置とを有するデータ処理機器。

【請求項 3 3】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第 1 のデータ処理装置と、

前記演算処理装置あるいは前記第 1 のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第 1 のデータ処理装置のスレーブとなって、前記第 1 のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第 2 のデータ処理装置と

を有するデータ処理機器。

【請求項 3 4】

前記演算処理装置、前記第 1 のデータ処理装置および前記第 2 のデータ処理装置を接続するバス

をさらに有する請求項 3 3 に記載のデータ処理機器。

【請求項 3 5】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、
前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第 1 のデータ処理装置と、

前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第 2 のデータ処理装置と
を有するデータ処理機器。

【請求項 3 6】

前記第 2 のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う

請求項 3 5 に記載のデータ処理機器。

【請求項 3 7】

前記第 2 のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う

請求項 3 5 に記載のデータ処理機器。

【請求項 3 8】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、
前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第 1 のデータ処理装置と、

前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第 2 のデータ処理装置と

を有するデータ処理機器。

【請求項 3 9】

前記第 1 のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを一時的に記憶し、当該記憶したコンテンツデータを前記第 2 のデータ処理装置に出力する記憶回路

をさらに有する請求項 3 8 に記載のデータ処理機器。

【請求項 4 0】

前記記憶回路は、耐振動用記憶回路の記憶領域の一部をその記憶領域とする請求項 3 9 に記載のデータ処理機器。

【請求項 4 1】

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第 3 のデータ処理装置

をさらに有する請求項 3 8 に記載のデータ処理機器。

【請求項 4 2】

演算処理装置およびデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記データ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性の回路モジュール内で、権利書データが示す取り扱いに基づいて、当該権利書データに対応したコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定の結果を示す履歴データを生成し、前記コンテンツ鍵データを復号する

データ処理方法。

【請求項 4 3】

前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、

前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指

定された処理に対応する割り込みルーチンを実行する

請求項 4 2 に記載のデータ処理方法。

【請求項 4 4】

前記データ処理装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する

請求項 4 2 に記載のデータ処理機器。

【請求項 4 5】

前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、

前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る

請求項 4 2 に記載のデータ処理方法。

【請求項 4 6】

前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示す第 1 のステータスレジスタのフラグを設定し、

前記演算処理装置は、前記第 1 のステータスレジスタのフラグから、前記データ処理装置の処理の実行状態を把握し、

前記演算処理装置は、前記データ処理装置に前記割り込みによって処理を依頼したことを示す第 2 のステータスレジスタのフラグに設定し、

前記データ処理装置は、前記第 2 のステータスレジスタのフラグから、前記演算処理装置が前記割り込みによって処理を依頼したか否かを把握する

請求項 4 5 に記載のデータ処理方法。

【請求項 4 7】

前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる

請求項 4 2 に記載のデータ処理方法。

【請求項 4 8】

前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツ

データの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する

請求項 4 2 に記載のデータ処理方法。

【請求項 4 9】

前記演算処理装置は、所定のユーザプログラムを実行する

請求項 4 2 に記載のデータ処理方法。

【請求項 5 0】

演算処理装置、第 1 のデータ処理装置および第 2 のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第 1 のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、

前記第 2 のデータ処理装置は、前記演算処理装置あるいは前記第 1 のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第 1 のデータ処理装置のスレーブとなって、耐タンパ性のモジュール内で、前記第 1 のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う

データ処理方法。

【請求項 5 1】

演算処理装置、第 1 のデータ処理装置および第 2 のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第 1 のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、

コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、

前記第 2 のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う

データ処理方法。

【請求項 5 2】

前記第 2 のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う

請求項 5 1 に記載のデータ処理方法。

【請求項 5 3】

前記第 2 のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う

請求項 5 1 に記載のデータ処理方法。

【請求項 5 4】

演算処理装置、第 1 のデータ処理装置および第 2 のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第 1 のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行い、

前記第 2 のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う

データ処理方法。

【請求項 5 5】

前記第 1 のデータ処理装置が前記記録媒体から読み出した前記コンテンツデー

タを記憶回路に一時的に記憶し、当該記憶回路から読み出したコンテンツデータを前記第 2 のデータ処理装置に出力する

請求項 5 4 に記載のデータ処理方法。

【請求項 5 6】

前記記憶回路として、耐振動用記憶回路の記憶領域の一部をその記憶領域を用いる

請求項 5 5 に記載のデータ処理方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、提供されたコンテンツデータに関連する処理を行うデータ処理装置、データ処理機器およびその方法に関する。

【0 0 0 2】

【従来の技術】

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来の EMD (Electronic Music Distribution: 電子音楽配信) システムがある。

【0 0 0 3】

図 1 0 6 は、従来の EMD システム 7 0 0 の構成図である。

図 1 0 6 に示す EMD システム 7 0 0 では、コンテンツプロバイダ 7 0 1 a, 7 0 1 b が、サービスプロバイダ 7 1 0 に対し、コンテンツデータ 7 0 4 a, 7 0 4 b, 7 0 4 c と、著作権情報 7 0 5 a, 7 0 5 b, 7 0 5 c とを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報 7 0 5 a, 7 0 5 b, 7 0 5 c には、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ 7 1 0 の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】

サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵データを用いて復号する。

そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツデータ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報をコンテンツデータ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。

さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA(Conditional Access)モジュール711に送信する。

【0005】

CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。

このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した

後に、サービスプロバイダ 710 の権利処理モジュール 720 に送信する。

この場合に、CA モジュール 711 は、サービスプロバイダ 710 が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】

サービスプロバイダ 710 は、CA モジュール 711 から課金情報 721 を受信すると、サービスプロバイダ 710 とコンテンツプロバイダ 701a, 701b, 701c との間で利益配分を行う。

このとき、サービスプロバイダ 710 から、コンテンツプロバイダ 701a, 701b, 701c への利益配分は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRAC によって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】

また、端末装置 709 では、コンテンツ鍵データ Kca, Kcb, Kcc を用いて復号したコンテンツデータ 707a, 707b, 707c を、RAM 型の記録媒体 723 などに記録する際に、著作権情報 705a, 705b, 705c の SCMS ビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ 707a, 707b, 707c に埋め込まれた SCMS ビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】

ところで、SCMS は、コンテンツデータを例えば 2 世代以上のわたって複製することを禁止するものであり、1 世代の複製は無制限に行うことができ、著作権者の保護として不十分であるという問題がある。

【0009】

また、上述した EMD システム 700 では、サービスプロバイダ 710 が暗号

化されていないコンテンツデータを技術的に自由に扱えるため、コンテンツプロバイダ 7 0 1 の関係者はサービスプロバイダ 7 1 0 の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ 7 0 1 の利益が不当に損なわれる可能性が高いという問題がある。

また、上述した EMD システム 7 0 0 では、ユーザの端末装置 7 0 9 がサービスプロバイダ 7 1 0 から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ 7 0 1 の利益が不当に損なわれるという問題がある。

【 0 0 1 0 】

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護するシステムおよび方法に適用可能なデータ処理装置、データ処理機器およびその方法を提供することを目的とする。

また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減するシステムおよび方法に適用可能なデータ処理装置、データ処理機器およびその方法を提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

上述した目的を達成するために、本発明の第 1 の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置であって、第 1 のバスと、前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第 1 のバスに接続された演算処理回路と、前記第 1 のバスに接続された記憶回路と、第 2 のバスと、前記第 1 のバスと前記第 2 のバスとの間に介在するインターフェイス回路と、前記第 2 のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、前記第 2 のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有する。

【 0 0 1 2 】

本発明の第 1 の観点のデータ処理装置では、例えば、コンテンツデータおよびそれに対応したコンテンツ鍵データおよび権利書データが配給と、暗号化された

コンテンツ鍵データを復号するライセンス鍵データが配給される。

ここで、ライセンス鍵データは、例えば、前記記憶回路に記憶される。

そして、例えば、外部バスインターフェイス回路を介して、外部の演算処理装置から権利処理などを行う指示が出されると、前記演算処理回路において、権利書データに基づいたコンテンツデータの権利処理が行われる。

その後、暗号処理回路において、記憶回路から読み出したライセンス鍵データを用いて、コンテンツ鍵データの復号が行われる。

そして、第 1 の観点のデータ処理装置は、他の復号装置との間で互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記復号したコンテンツ鍵データおよびコンテンツデータを暗号化し、当該暗号化したコンテンツ鍵データおよびコンテンツデータを前記他の復号装置に送る。

【0013】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記インターフェイス回路を第 1 のインターフェイス回路とした場合に、前記第 1 のバスは、前記演算処理回路および前記記憶回路に接続された第 3 のバスと、前記第 1 のインターフェイス回路に接続された第 4 のバスとを有し、前記データ処理装置は、

前記第 3 のバスと前記第 4 のバスとの間に介在する第 2 のインターフェイス回路を前記耐タンパ性の回路モジュール内にさらに有する。

【0014】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、第 5 のバスと、記録媒体または IC カードに搭載された認証機能を持つデータ処理回路との間の通信処理を行い、前記第 5 のバスに接続された第 3 のインターフェイス回路と、前記第 4 のバスと前記第 5 のバスとの間に介在する第 4 のインターフェイス回路とを前記耐タンパ性の回路モジュール内にさらに有する。

【0015】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記暗号処理回路は、公開鍵暗号回路と、共通鍵暗号回路とを有する。

【0016】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記記憶回路は

、当該データ処理装置の秘密鍵データおよび他の装置の公開鍵データを記憶し、前記公開鍵暗号回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する前記公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成し、前記共通鍵暗号回路は、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する。

【 0 0 1 7 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路を前記耐タンパ性の回路モジュール内にさらに有し、前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う。

【 0 0 1 8 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該他の装置との間の相互認証を行うために乱数を生成し、前記第 2 のバスに接続された乱数生成回路を前記耐タンパ性の回路モジュール内にさらに有する。

【 0 0 1 9 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイス回路は、当該データ処理装置が搭載された機器の制御を統括的に行うホスト演算処理装置に接続される。

【 0 0 2 0 】

また、本発明の第 1 の観点のデータ処理装置は、前記演算処理回路は、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する。

【 0 0 2 1 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記演算処理回路は、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成し、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する。

【 0 0 2 2 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記共通鍵暗号回路は、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する。

【 0 0 2 3 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する。

【 0 0 2 4 】

また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記記憶回路は、ブロック単位でデータの書き込みおよび消去が行われ、前記演算処理回路によって制御され、前記記憶回路に対してのデータの書き込みおよび消去の許否を前記ブロック単位で管理する書き込みロック制御回路を前記耐タンパ性の回路モジュール内にさらに有する。

【 0 0 2 5 】

また、本発明の第 2 の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置であって、第 1 のバスと、前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第 1 のバスに接続された演算処理回路と、前記第 1 のバスに接続された記憶回路と、第 2 のバスと、前記第 1 のバスと前記第 2 のバスとの間に介在するインターフェイス回路と、前記第 2 のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、前記第 2 のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有し、前記演算処理回路は、前記外部バスインターフェイス回路を介して外部回路から割り込みを受けると、当該外部回路のスレーブとなって当該割り込みによって指定された処理を行い、当該処理の結果を前記外部装置に通知する。

【 0 0 2 6 】

また、本発明の第 2 の観点のデータ処理装置は、好ましくは、前記演算処理回路は、前記処理の結果を前記外部回路に割り込みを出して通知する。

【 0 0 2 7 】

また、本発明の第 2 の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイスは、前記演算処理回路および前記外部回路との共有メモリを有し、前記演算処理回路は、当該共有メモリに前記処理の結果を書き込み、当該処理の結果は前記外部回路からのポーリングによって当該外部回路に通知される。

【 0 0 2 8 】

また、本発明の第 2 の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイスは、前記外部回路から依頼された処理の前記演算処理回路における実行状態を示し、前記演算処理回路によって設定され、前記外部回路によって読まれるフラグを持つ第 1 のステータスレジスタと、前記外部回路が前記演算処理回路に処理を依頼したか否かを示し、前記外部回路によって設定され、前記演算処理回路によって読まれるフラグを持つ第 2 のステータスレジスタと、前記処理の結果が書き込まれる記憶回路とを有する。

【 0 0 2 9 】

また、本発明の第 2 の観点のデータ処理装置は、好ましくは、前記記憶回路は、前記割り込みによって指定される処理を記述した割り込みプログラムを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行して前記処理を行う。

【 0 0 3 0 】

また、本発明の第 2 の観点のデータ処理装置は、好ましくは、前記記憶回路は、複数の前記割り込みプログラムと、当該割り込みプログラムを実行する際に読み出される複数のサブルーチンを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行する際に、前記記憶回路から必要に応じて前記サブルーチンを読み出して実行する。

【 0 0 3 1 】

また、本発明の第 1 の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置と有するデータ処理機器であって、前記データ処理装置は、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【 0 0 3 2 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する。

【 0 0 3 3 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記データ処理

装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する。

【 0 0 3 4 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る。

【 0 0 3 5 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示し、前記演算処理装置によって読まれるフラグを持つ第 1 のステータスレジスタと、前記演算処理装置が当該データ処理装置に前記割り込みによって処理を依頼したか否かを示し、前記演算処理装置によって設定されるフラグを持つ第 2 のステータスレジスタと、前記処理の結果が書き込まれる前記共有メモリとを有する。

【 0 0 3 6 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる。

【 0 0 3 7 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する。

【 0 0 3 8 】

また、本発明の第 1 の観点のデータ処理機器は、好ましくは、前記演算処理装置は、所定のユーザプログラムを実行する。

【 0 0 3 9 】

また、本発明の第 2 の観点のデータ処理機器は、データ提供装置が提供したコ

コンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理機器であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第 1 の処理モジュールと、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置であって、前記受信したモジュールに格納された権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納されたコンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置とを有する。

【 0 0 4 0 】

また、本発明の第 3 の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第 1 のデータ処理装置と、前記演算処理装置あるいは前記第 1 のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第 1 のデータ処理装置のスレーブとなって、前記第 1 のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第 2 のデータ処理装置とを有する。

【 0 0 4 1 】

また、本発明の第 4 の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第 1 のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第 2 のデータ処理装置とを有する。

【 0 0 4 2 】

また、本発明の第 4 の観点のデータ処理機器は、好ましくは、前記第 2 のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う。

【 0 0 4 3 】

また、本発明の第 4 の観点のデータ処理機器は、好ましくは、前記第 2 のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う。

【 0 0 4 4 】

また、本発明の第 5 の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第 1 のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第 2 のデータ処理装置とを有する。

【 0 0 4 5 】

また、本発明の第 5 の観点のデータ処理機器は、好ましくは、前記第 1 のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを一時的に記憶

し、当該記憶したコンテンツデータを前記第 2 のデータ処理装置に出力する記憶回路をさらに有する。

【0046】

また、本発明の第 5 の観点のデータ処理機器は、好ましくは、前記記憶回路は、耐振動用記憶回路の記憶領域の一部をその記憶領域とする。

【0047】

また、本発明の第 5 の観点のデータ処理装置は、好ましくは、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第 3 のデータ処理装置をさらに有する。

【0048】

また、本発明の第 1 の観点のデータ処理方法は、演算処理装置およびデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記データ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性の回路モジュール内で、権利書データが示す取り扱いに基づいて、当該権利書データに対応したコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定の結果を示す履歴データを生成し、前記コンテンツ鍵データを復号する。

【0049】

また、本発明の第 2 の観点のデータ処理方法は、演算処理装置、第 1 のデータ処理装置および第 2 のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第 1 のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、前記第 2 のデータ処理装置は、前記演算処理装置あるいは前記第 1 のデータ処理装置から割り込みを受けて、マスタであ

る前記演算処理装置あるいは前記第 1 のデータ処理装置のスレーブとなって、耐タンパ性のモジュール内で、前記第 1 のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う。

【0050】

また、本発明の第 3 の観点のデータ処理方法は、演算処理装置、第 1 のデータ処理装置および第 2 のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第 1 のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、前記第 2 のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う。

【0051】

また、本発明の第 4 の観点のデータ処理方法は、演算処理装置、第 1 のデータ処理装置および第 2 のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第 1 のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行い、前記第 2 のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う。

【0052】

【発明の実施の形態】

以下、本発明の実施形態に係わる EMD (Electronic Music Distribution: 電

子音楽配信) システムについて説明する。

第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。

本実施形態において、ユーザに配信されるコンテンツ(Content) データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105₁~105₄が、本発明のデータ提供装置、管理装置およびデータ処理装置にそれぞれ対応している。

先ず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データK_c、コンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるEMDサービスセンタ102に送る。

【0053】

EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データK_c、権利書データ106並びに電子透かし情報鍵データを登録(認証および権威化)する。

また、EMDサービスセンタ102は、対応する期間のライセンス鍵データK_{D1}~K_{D56}で暗号化したコンテンツ鍵データK_c、権利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。

ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102にお

いて正規に登録されたことを検証するために用いられる。

【0054】

また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテンツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。

ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0055】

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁およびAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM(Secure Application Module)105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0056】

SAM105₁～105₄は、ネットワーク機器160₁がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および／または、コンテンツプロバイダ101からAV機器160₂～160₄に記録媒体を介してオフラインで供給されたセキュアコンテナ104に対応する期間のライセンス鍵データKD₁～KD₃を用いて復号した後に、署名データの検証を行う。

SAM105₁～105₄に供給されたセキュアコンテナ104は、ネットワ

ーク機器 160₁ および AV 機器 160₂ ~ 160₄ において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM105₁ ~ 105₄ は、上述したセキュアコンテナ 104 の購入・利用の履歴を利用履歴 (Usage Log) データ 108 として記録すると共に、購入形態を示す利用制御データ 166 を作成する。

利用履歴データ 108 は、例えば、EMD サービスセンタ 102 からの要求に応じて、ユーザホームネットワーク 103 から EMD サービスセンタ 102 に送信される。

利用制御データ 166 は、例えば、購入形態が決定される度に、ユーザホームネットワーク 103 から EMD サービスセンタ 102 に送信される。

【0057】

EMD サービスセンタ 102 は、利用履歴データ 108 に基づいて、課金内容を決 (計算) し、その結果に基づいて、ペイメントゲートウェイ 90 を介して銀行などの決済機関 91 に決済を行なう。これにより、ユーザホームネットワーク 103 のユーザが決済機関 91 に支払った金銭が、EMD サービスセンタ 102 による決済処理によって、コンテンツプロバイダ 101 に支払われる。

また、EMD サービスセンタ 102 は、一定期間毎に、決済レポートデータ 107 をコンテンツプロバイダ 101 に送信する。

【0058】

本実施形態では、EMD サービスセンタ 102 は、認証機能、鍵データ管理機能および権利処理 (利益分配) 機能を有している。

すなわち、EMD サービスセンタ 102 は、中立の立場にある最高の権威機関であるルート認証局 92 に対しての (ルート認証局 92 の下層に位置する) セカンド認証局 (Second Certificate Authority) としての役割を果たし、コンテンツプロバイダ 101 および SAM105₁ ~ 105₄ において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMD サービスセンタ 102 の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMD サービスセンタ 102 は、コンテンツプ

ロバイダ 101 の権利書データ 106 を登録して権威化することも、EMD サービスセンタ 102 の認証機能の一つである。

また、EMD サービスセンタ 102 は、例えば、ライセンス鍵データ $KD_1 \sim KD_6$ などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMD サービスセンタ 102 は、権威化した権利書データ 106 に記述された標準小売価格 SRP (Suggested Retailer' Price) と SAM105₁ ~ SAM105₄ から入力した利用履歴データ 108 とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ 101 に分配する権利処理（利益分配）機能を有する。

【0059】

図 2 は、セキュアコンテナ 104 の概念をまとめた図である。

図 2 に示すように、セキュアコンテナ 104 には、コンテンツプロバイダ 101 が作成したコンテンツファイル CF と、EMD サービスセンタ 102 が作成したキーファイル KF とが格納されている。

コンテンツファイル CF には、ヘッダ部およびコンテンツ ID を含むヘッダデータと、コンテンツ鍵データ K_c を用いた暗号化されたコンテンツデータ C と、これらについてのコンテンツプロバイダ 101 の秘密鍵データ $K_{CP,S}$ を用いた署名データとが格納されている。

キーファイル KF には、ヘッダ部およびコンテンツ ID を含むヘッダデータと、ライセンス鍵データ $KD_1 \sim KD_6$ によって暗号化されたコンテンツ鍵データ K_c および権利書データ 106 と、これらについての EMD サービスセンタ 102 の秘密鍵データ $K_{ESC,S}$ による署名データとが格納されている。

なお、図 2 において、権利書データ 106 は、ライセンス鍵データによって暗号化されていなくてもよい。但し、この場合でも、権利書データ 106 には、コンテンツプロバイダ 101 の秘密鍵データ $K_{CP,S}$ を用いた署名データを付加する。

【0060】

以下、EMD システム 100 の各構成要素について詳細に説明する。

〔コンテンツプロバイダ 101〕

コンテンツプロバイダ 101 は、EMD サービスセンタ 102 との間で通信を行う前に、例えば、自らが生成した公開鍵データ $K_{CP,P}$ 、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインで EMD サービスセンタ 102 に登録し、自らの識別子（識別番号） CP_ID を得る。また、コンテンツプロバイダ 101 は、EMD サービスセンタ 102 から、EMD サービスセンタ 102 の公開鍵データ $K_{ESC,P}$ と、ルート認証局 92 の公開鍵データ $K_{R-CA,P}$ とを受ける。

【0061】

コンテンツプロバイダ 101 は、図 3 (A) に示すコンテンツファイル CF と、当該コンテンツファイル CF の署名データ $SIG_{6,CP}$ と、キーファイルデータベース 118b から読み出した当該コンテンツファイル CF に対応する図 3 (B) に示すキーファイル KF と、当該キーファイル KF の署名データ $SIG_{7,CP}$ と、記憶部 119 から読み出したコンテンツプロバイダ 101 の公開鍵証明書データ CER_{CP} と、当該公開鍵証明書データ CER_{CP} の署名データ $SIG_{1,ESC}$ とを格納したセキュアコンテナ 104 を生成する。

また、コンテンツプロバイダ 101 は、セキュアコンテナ 104 をオンラインあるいはオフラインで、図 1 に示すユーザホームネットワーク 103 のネットワーク機器 160₁ に供給する。

このように、本実施形態では、コンテンツプロバイダ 101 の公開鍵データ $K_{CP,P}$ の公開鍵証明書 CER_{CP} をセキュアコンテナ 104 に格納してユーザホームネットワーク 103 に送信するイン・バンド (In-band) 方式を採用している。従って、ユーザホームネットワーク 103 は、公開鍵証明書 CER_{CP} を得るための通信を EMD サービスセンタ 102 との間で行う必要がない。

なお、本発明では、公開鍵証明書 CER_{CP} をセキュアコンテナ 104 に格納しないで、ユーザホームネットワーク 103 が EMD サービスセンタ 102 から公開鍵証明書 CER_{CP} を得るアウト・オブ・バンド (Out-of-band) 方式を採用してもよい。

【0062】

なお、本実施形態では、署名データは、コンテンツプロバイダ 101、EMD

サービスセンタ 1 0 2 および SAM 1 0 5₁ ～ 1 0 5₄ の各々において、署名を行なう対象となるデータのハッシュ値をとり、自らの秘密鍵データ $K_{CP,S}$ 、 K_{ES_C} 、 K_{SAM1} ～ K_{SAM4} を用いて作成される。ここで、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【 0 0 6 3 】

以下、セキュアコンテナ 1 0 4 内の各データについて詳細に説明する。

＜署名データ SIG_{6,CP}＞

署名データ SIG_{6,CP} は、セキュアコンテナ 1 0 4 の受信先において、コンテンツファイル CF の作成者および送信者の正当性を検証するために用いられる。

＜署名データ SIG_{7,CP}＞

署名データ SIG_{7,CP} は、セキュアコンテナ 1 0 4 の受信先において、キーファイル KF の送信者の正当性を検証するために用いられる。なお、セキュアコンテナ 1 0 4 の受信先において、キーファイル KF の作成者の正当性の検証は、キーファイル KF 内の署名データ SIG_{K1,ESC} に基づいて行われる。また、署名データ SIG_{K1,ESC} は、キーファイル KF が、EMD サービスセンタ 1 0 2 に登録されているか否かを検証するためにも用いられる。

【 0 0 6 4 】

＜コンテンツファイル CF＞

図 4 は、図 3（A）に示すコンテンツファイル CF をさらに詳細に説明するための図である。

コンテンツファイル CF は、図 3（A）および図 4 に示すように、ヘッダデータと、暗号化部 1 1 4 から入力したそれぞれコンテンツ鍵データ K_c で暗号化されたメタデータ Meta、コンテンツデータ C、A/V 伸長用ソフトウェア Soft および電子透かし情報モジュール (Watermark Module) WM とを格納している

。なお、図3(A)は、コンテンツデータCを伸長するAV圧縮伸長用装置として、DSP(Digital Signal Processor)を用いた場合のコンテンツファイルCFの構成である。当該DSPでは、セキュアコンテナ104内のA/V伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ104内のコンテンツデータCの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ101は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。

AV圧縮伸長用装置としてA/V伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルCF内にA/V伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【0065】

ヘッダデータには、図4に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データ $K_{CP,S}$ による署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルCFの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関する情報、およびディレクトリ情報などに関するコンテンツプロバイダ101の秘密鍵データ $K_{CP,S}$ による署名データが含まれる。

【0066】

メタデータMetaには、図4に示すように、商品(コンテンツデータC)の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ101による署名データが含まれる。

本発明では、図3(A)および図4に示すように、コンテンツファイルCF内にメタデータMetaを格納して送信する場合を例示するが、メタデータMetaをコンテンツファイルCF内に格納せずに、コンテンツファイルCFを送信する経路とは別の経路でコンテンツプロバイダ101からSAM105₁などに送信してもよい。

【0067】

コンテンツデータCは、例えば、コンテンツマスターソースデータベースから読み出したコンテンツデータに対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wc、ユーザ電子透かし情報(User Watermark)Wuおよびリンク用電子透かし情報(Link Watermark)WLなどを埋め込んだ後に、例えば、ATRAC3(Adaptive Transform Acoustic Coding 3)(商標)などの音声圧縮方式で圧縮され、その後、コンテンツ鍵データKcを共通鍵として用い、DES(Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で暗号化されたデータである。

ここで、コンテンツ鍵データKcは、例えば、乱数発生器を用いて所定ビット数の乱数を発生して得られる。なお、コンテンツ鍵データKcは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。

また、複数のコンテンツプロバイダ101が存在する場合に、個々のコンテンツプロバイダ101によって固有のコンテンツ鍵データKcを用いてもよいし、全てのコンテンツプロバイダ101に共通のコンテンツ鍵データKcを用いてもよい。

【0068】

ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。

コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。

ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM105₁~105₄の識別子SAM_ID₁~SAM_ID₄が含まれる。

リンク用電子透かし情報(Link Watermark)WLは、例えば、コンテンツデータCのコンテンツIDを含んでいる。

リンク用電子透かし情報WLをコンテンツデータCに埋め込むことで、例えば、テレビジョンやAM/FMラジオなどのアナログ放送でコンテンツデータCが配信された場合でも、ユーザからの要求に応じて、EMDサービスセンタ102は、当該コンテンツデータCを扱っているコンテンツプロバイダ101をユーザに紹介できる。すなち、当該コンテンツデータCの受信先において、電子透かし情報デコーダを利用したコンテンツデータCに埋め込まれたリンク用電子透かし情報WLを検出し、当該検出したリンク用電子透かし情報WLに含まれるコンテンツIDをEMDサービスセンタ102に送信することで、EMDサービスセンタ102は当該ユーザに対して、当該コンテンツデータCを扱っているコンテンツプロバイダ101などを紹介できる。

【0069】

具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータCに埋め込まれているリンク用電子透かし情報WLに含まれるコンテンツIDや当該コンテンツデータCを登録しているEMDサービスセンタ102の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやMD(Mini Disk)などの光ディスクなどの可搬メディアに搭載されているメディアSAMに記録する。そして、当該可搬メディアをネットワークに接続されているSAMを搭載したネットワーク機器をセットする。そして、当該SAMとEMDサービスセンタ102とが相互認証を行った後に、メディアSAMに搭載されている個人情報と、上記記録したコンテンツIDなどをネットワーク機器からEMDサービスセンタ102に送信する。その後、ネットワーク機器に、当該コンテンツデータCを扱っているコンテンツプロバイダ101などの紹介リストなどを、EMDサービスセンタ102から受信する。

また、その他に、例えば、EMDサービスセンタ102が、ユーザからコンテンツIDなどを受信したときに、当該コンテンツIDに対応したコンテンツデータCを提供しているコンテンツプロバイダ101に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ101は

、当該ユーザが契約者であれば、当該コンテンツデータCをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【0070】

なお、後述する第2実施形態では、リンク用電子透かし情報WLに基づいて、EMDサービスセンタ302は、ユーザに、当該コンテンツデータCを扱っているサービスプロバイダ310を紹介できる。

【0071】

また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、EMDサービスセンタ102において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク103内のネットワーク機器160₁ およびAV機器160₂ ~ 160₄ が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク103では、EMDサービスセンタ102が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0072】

A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器160₁ およびAV機器160₂ ~ 160₄ において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の伸長用ソフトウェアである。

このように、セキュアコンテナ104内にA/V伸長用ソフトウェアSoftを格納することで、SAM105₁ ~ 105₄ においてセキュアコンテナ104内に格納されたA/V伸長用ソフトウェアSoftを用いてコンテンツデータCの伸長を行うことができ、コンテンツデータC毎あるいはコンテンツプロバイダ101毎にコンテンツデータCの圧縮および伸長方式をコンテンツプロバイダ1

0 1 が自由に設定しても、ユーザに多大な負担をかけることはない。

【 0 0 7 3 】

また、コンテンツファイル C F には、図 4 に示すように、ファイルリーダーと、秘密鍵データ $K_{cp,S}$ によるファイルリーダーの署名データとを含むようにしてもよい。このようにすることで、 $SAM105_1 \sim 105_4$ において、異系列の複数のセキュアコンテナ 1 0 4 から受信したそれぞれ異なるフォーマットのコンテンツファイル C F を格納した複数のセキュアコンテナ 1 0 4 を効率的に処理できる。

【 0 0 7 4 】

ここで、ファイルリーダーは、コンテンツファイル C F およびそれに対応するキーファイル K F を読む際に用いられ、これらのファイルの読み込み手順などを示している。

但し、本実施形態では、EMD サービスセンタ 1 0 2 から $SAM105_1 \sim 105_4$ に、当該ファイルリーダーを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ 1 0 4 のコンテンツファイル C F は、ファイルリーダーを格納していない。

【 0 0 7 5 】

本実施形態では、コンテンツデータ C の圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータ C を得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータ C がセキュアコンテナ 1 0 4 内に格納されている。すなわち、これらの事項をコンテンツプロバイダ 1 0 1 が自由に決定できる。

【 0 0 7 6 】

< キーファイル K F >

図 5 は、図 3（A）に示すキーファイル K F を詳細に説明するための図である。

本実施形態では、例えば、図 6 に示すように、コンテンツプロバイダ 1 0 1 から EMD サービスセンタ 1 0 2 に登録用モジュール Mod_2 が送られて登録処理

が行われた後に、例えば6カ月分のキーファイルKFがEMDサービスセンタ102からコンテンツプロバイダ101に送られ、キーファイルデータベースに格納される。このとき、登録用モジュールMod₂ およびキーファイルKFの送受信時に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証およびセッション鍵データK_{SES} による暗号化および復号が行われる。

キーファイルKFは、コンテンツデータC毎に存在し、後述するように、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSDによって、対応するコンテンツファイルCFとの間でリンク関係が指定されている。

キーファイルKFには、図3（B）および図5に示すように、ヘッダ、コンテンツ鍵データK_c、権利書データ（使用許諾条件）106、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃ および署名データSIG_{K1,ESC}が格納されている。

ここで、コンテンツプロバイダ101の秘密鍵データK_{ESC,S} を用いた署名データは、図3（B）に示すようにキーファイルKFに格納される全てのデータに対しての署名データK_{1,ESC}にしてもよいし、図5に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データK_cおよび権利書データ106に対しての署名データと、SAMプログラム・ダウンロード・コンテナSDCに対しての署名データとを別々に設けてもよい。

コンテンツ鍵データK_cおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃ とは、それぞれ対応する期間のライセンス鍵データKD₁～KD₆ を用いて暗号化されている。

なお、権利書データ106は、キーファイルKF内に格納しなくてもよい。この場合には、例えば、権利書データ106はライセンス鍵データによる暗号化を行わずに、署名データを付加する。

【0077】

ヘッダデータには、図5に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データK_{ESC,S} による署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルKFに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイ

ダ 101 の秘密鍵データ $K_{ESC,S}$ による署名データが含まれる。

なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図 7 に示すような情報を含めてもよい。

また、コンテンツ ID には、例えば、図 8 に示す情報が含まれている。コンテンツ ID は、EMD サービスセンタ 102 あるいはコンテンツプロバイダ 101 において作成され、EMD サービスセンタ 102 において作成された場合には図 8 に示すように EMD サービスセンタ 102 の秘密鍵データ $K_{ESC,S}$ による署名データが添付され、コンテンツプロバイダ 101 において作成された場合にはコンテンツプロバイダ 101 の秘密鍵データ $K_{CP,S}$ が添付される。

コンテンツ ID は、コンテンツプロバイダ 101 および EMD サービスセンタ 102 の何れで作成してもよい。

【0078】

ディレクトリ構造データは、セキュアコンテナ 104 内におけるコンテンツファイル CF 相互間の対応関係と、コンテンツファイル CF とキーファイル KF との対応関係を示している。

例えば、セキュアコンテナ 104 内にコンテンツファイル $CF_1 \sim CF_3$ と、それらに対応するキーファイル $KF_1 \sim KF_3$ が格納されている場合には、10 図 9 に示すように、コンテンツファイル $CF_1 \sim CF_3$ 相互間のリンクと、コンテンツファイル $CF_1 \sim CF_3$ とキーファイル $KF_1 \sim KF_3$ との間のリンク関係とがディレクトリ構造データによって確立される。

ハイパーリンクデータは、セキュアコンテナ 104 の内外の全てのファイルを対象として、キーファイル KF 相互間での階層構造と、コンテンツファイル CF とキーファイル KF との対応関係を示している。

具体的には、図 10 に示すように、セキュアコンテナ 104 内にコンテンツファイル CF およびキーファイル KF 毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数 $H(x)$ を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【0079】

また、権利書データ106は、コンテンツデータCの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ101の運用者が希望する卸売価格やコンテンツデータCの複製ルールなどが記述されている。

具体的には、権利書データ106には、図5に示すように、コンテンツID、コンテンツプロバイダ101の識別子CP_ID、権利書データ106の有効期限、EMDサービスセンタ102の通信アドレス、利用空間調査情報、卸売価格情報SRP (Suggested Retailer' Price)、取扱方針、取扱制御情報(Usage Control)、商品デモ（試聴）の取扱制御情報およびそれらについての署名データなどが含まれる。

ここで、取扱制御情報は、例えば、再配付(Re-Distribution)、再生課金(Pay Per Use)、完全買い切り(Sell Through)、時間制限買い切り(Time Limited Sell Through)、回数制限買い切り(Shell Through Pay Per Play N)、時間課金(Pay Per Time)、SCMS機器への再生課金、ブロック課金(Pay Per Block)などの購入形態のうち許諾された購入形態を示す情報である。

【0080】

なお、後述する第2実施形態のように、サービスプロバイダ310を介してユーザホームネットワーク303にセキュアコンテナ304を送信する場合には、権利書データ106には、コンテンツプロバイダ301がセキュアコンテナ104を提供するサービスプロバイダ310の識別子SP_IDが含まれる。

【0081】

また、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃には、図5に示すように、SAM105₁～105₄内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ(UCP)U106のシンタックス（文法）を示すUCP-L(Label)、R(Reader)などのラベルリーダーと、SAM105₁～105₄に内蔵された記憶部192（マスクROM1104、不揮発性メモリ1105などのフラッシュユーROM）の書き換えおよび消去をブロック単位でロック状態／非ロック状態

にするためのロック鍵データと、それらについての署名データとが含まれる。S
AM105₁ ~ 105₄ のマスクROM1104および不揮発性メモリ1105
では、ロック鍵データに基づいて、記憶データの書き換えおよび消去を許可する
か否かをブロック単位で制御する。

【0082】

以下、コンテンツプロバイダ101からユーザホームネットワーク103にセ
キュアコンテナ104を供給する形態について説明する。

コンテンツプロバイダ101は、前述したように、セキュアコンテナ104を
、オフラインおよび／またはオンラインでユーザホームネットワーク103に供
給する。

コンテンツプロバイダ101は、オンラインで、セキュアコンテナ104をユ
ーザホームネットワーク103のネットワーク機器160₁ に供給する場合には
、ネットワーク機器160₁ との間で相互認証を行ってセッション鍵（共通鍵）
データK_{SES} を共有し、セキュアコンテナ104を当該セッション鍵データK_{SE}
S を用いて暗号化してEMDサービスセンタ102に送信する。セッション鍵デ
ータK_{SES} は、相互認証を行う度に新たに生成される。

このとき、セキュアコンテナ104を送信する通信プロトコルとして、デジ
タル放送であればMHEG (Multimedia and Hypermedia information coding Ex
perts Group) プロトコルを用い、インターネットであればXML／SMIL／H
TML (Hyper TextMarkup Language) を用い、これらの通信プロトコル内に、セ
キュアコンテナ104を、符号化方式に依存しない形式でトンネリングして埋め
込む。

従って、通信プロトコルとセキュアコンテナ104との間でフォーマットの整
合性をとる必要性はなく、セキュアコンテナ104のフォーマットを柔軟に設定
できる。

なお、コンテンツプロバイダ101からユーザホームネットワーク103にセ
キュアコンテナ104を送信する際に用いる通信プロトコルは、上述したもの
には限定されず任意である。

本実施形態では、コンテンツプロバイダ101、EMDサービスセンタ102

およびネットワーク機器 1 6 0₁ に内蔵された相互間で通信を行うためのモジュールとして、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【 0 0 8 3 】

また、コンテンツプロバイダ 1 0 1 は、オフラインで、セキュアコンテナ 1 0 4 をユーザホームネットワーク 1 0 3 に供給する場合には、以下に示すような ROM 型あるいは RAM 型の記録媒体にセキュアコンテナ 1 0 4 を記録して、当該記録媒体を所定の流通経路を経てユーザホームネットワーク 1 0 3 に供給する。

図 1 1 は、本実施形態で用いられる ROM 型の記録媒体 1 3 0₁ を説明するための図である。

図 1 1 に示すように、ROM 型の記録媒体 1 3 0₁ は、ROM 領域 1 3 1、セキュア RAM 領域 1 3 2 およびメディア SAM 1 3 3 を有する。

ROM 領域 1 3 1 には、図 3 (A) に示したコンテンツファイル CF が記憶されている。

また、セキュア RAM 領域 1 3 2 は、記憶データに対してのアクセスに所定の許可（認証）が必要な領域であり、図 3 (B)、(C) に示したキーファイル KF および公開鍵証明書データ CER_{CP} と機器の種類に応じて固有の値を持つ記録用鍵データ K_{STR} とを引数として MAC (Message Authentication Code) 関数を用いて生成した署名データと、当該キーファイル KF および公開鍵証明書データ CER_{CP} とを記録媒体に固有の値を持つメディア鍵データ K_{MED} を用いて暗号化したデータとが記憶される。

また、セキュア RAM 領域 1 3 2 には、例えば、不正行為などで無効となったコンテンツプロバイダ 1 0 1 および SAM 1 0 5₁ ~ 1 0 5₅ を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

本実施形態で用いられるメディア SAM および後述するメディア・ドラブ SAM 2 6 0 では、これら相互間で通信を行う際に、自らが持つリボケーションリストと相手方が持つリボケーションリストとの作成時を比較し、自らが持つリボケーションリストの作成時が前の場合には、相手方が持つリボケーションリストによって自らのリボケーションリストを更新する。

また、セキュアRAM領域132には、後述するようにユーザホームネットワーク103のSAM105₁～105₄においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御データ166がセキュアRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130₁となる。

メディアSAM133には、例えば、ROM型の記録媒体130₁の識別子であるメディアIDと、メディア鍵データK_{MED}とが記憶されている。

メディアSAM133は、例えば、相互認証機能を有している。

【0084】

本実施形態で用いるROM型の記録媒体としては、例えば、図11に示すものの他に、図12に示すROM型の記録媒体130₂および図13に示すROM型の記録媒体130₃なども考えられる。

図12に示すROM型の記録媒体130₂は、ROM領域131と認証機能を有するメディアSAM133とを有し、図11に示すROM型の記録媒体130₁のようにセキュアRAM領域132を備えていない。ROM型の記録媒体130₂を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。

また、図13に示すROM型の記録媒体130₃は、ROM領域131およびセキュアRAM領域132を有し、図11に示すROM型の記録媒体130₁のようにメディアSAM133を有していない。ROM型の記録媒体130₃を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、ROM型の記録媒体130₃を用いる場合には、SAMとの間で相互認証は行わない。

また、本実施形態ではROM型の記録媒体の他にRAM型の記録媒体も用いられる。

【0085】

本実施形態で用いるRAM型の記録媒体としては、例えば図14に示すように、メディアSAM133、セキュアRAM領域132およびセキュアでないRA

M領域 134 を有する RAM 型の記録媒体 130₄ がある。RAM 型の記録媒体 130₄ では、メディア SAM 133 は認証機能を持ち、キーファイル KF を記憶する。また、RAM 領域 134 には、コンテンツファイル CF が記録される。

また、本実施形態で用いる RAM 型の記録媒体としては、その他に、図 15 に示す RAM 型の記録媒体 1350₅ および図 16 に示す RAM 型の記録媒体 130₆ なども考えられる。

図 15 に示す RAM 型の記録媒体 130₅ は、セキュアでない RAM 領域 134 と認証機能を有するメディア SAM 133 とを有し、図 14 に示す RAM 型の記録媒体 130₄ のようにセキュア RAM 領域 132 を備えていない。RAM 型の記録媒体 130₅ を用いる場合には、RAM 領域 134 にコンテンツファイル CF を記録し、メディア SAM 133 にキーファイル KF を記憶する。

また、図 16 に示す RAM 型の記録媒体 130₆ は、セキュア RAM 領域 132 およびセキュアでない RAM 領域 134 を有し、図 14 に示す RAM 型の記録媒体 130₄ のようにメディア SAM 133 を有していない。RAM 型の記録媒体 130₆ を用いる場合には、RAM 領域 134 にコンテンツファイル CF を記録し、セキュア RAM 領域 132 にキーファイル KF を記録する。また、RAM 型の記録媒体 130₆ を用いる場合には、SAM との間で相互認証は行わない。

【0086】

ここで、コンテンツプロバイダ 101 からユーザホームネットワーク 103 へのコンテンツデータ C の配給は、上述したように記録媒体 130₁ を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ 106 が格納された共通の形式のセキュアコンテナ 104 を用いる。従って、ユーザホームネットワーク 103 の SAM 105₁ ~ 105₄ では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ 106 に基づいた権利処理を行なうことができる。

【0087】

また、上述したように、本実施形態では、セキュアコンテナ 104 内に、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C と、当該暗号化を解くためのコンテンツ鍵データ Kc とを同封するイン・バンド (In-Band) 方式を採用し

ている。イン・バンド方式では、ユーザホームネットワーク 103 の機器で、コンテンツデータ C を再生しようとするときに、コンテンツ鍵データ Kc を別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データ Kc はライセンス鍵データ KD₁ ~ KD₆ で暗号化されているが、ライセンス鍵データ KD₁ ~ KD₆ は、EMD サービスセンタ 102 で管理されており、ユーザホームネットワーク 103 の SAM105₁ ~ 105₅ に事前に (SAM105₁ ~ 105₄ が EMD サービスセンタ 102 に初回にアクセスする際に) 配信されているので、ユーザホームネットワーク 103 では、EMD サービスセンタ 102 との間をオンラインで接続することなく、オフラインで、コンテンツデータ C の利用が可能になる。

なお、本発明は、後述するようにコンテンツデータ C とコンテンツ鍵データ Kc とを別々に、ユーザホームネットワーク 103 に供給するアウト・オブ・バンド (Out-Of-Band) 方式を採用できる柔軟性を有している。

【0088】

以下、コンテンツプロバイダ 101 におけるセキュアコンテナ 104 の作成に係わる処理の流れを説明する。

図 17, 図 18, 図 19 は、当該処理の流れを説明するためのフローチャートである。

ステップ S17-1: コンテンツプロバイダ 101 の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMD サービスセンタ 102 に登録処理を行い、グローバルユニークな識別子 CP_ID を得ている。また、コンテンツプロバイダ 101 は、予め自らの公開鍵証明書データ CER_{CP} を EMD サービスセンタ 102 から得ている。

ステップ S17-2: コンテンツプロバイダ 101 は、新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスターソースをデジタル化し、さらにコンテンツ ID を割り振り、コンテンツマスターソースデータベースに格納して一元的に管理する。

ステップ S17-3: コンテンツプロバイダ 101 は、ステップ S17-2 において一元的に管理した各々のコンテンツマスターソースにメタデータ Meta を

作成し、これをメタデータベースに格納して管理する。

【0089】

ステップ S17-4 : コンテンツプロバイダ 101 は、コンテンツマスターデータベースからコンテンツマスターソースであるコンテンツデータを読み出して電子透かし情報を埋め込む。

ステップ S17-5 : コンテンツプロバイダ 101 は、ステップ S17-4 で埋め込んだ電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップ S17-6 : 電子透かし情報が埋め込まれたコンテンツデータを圧縮する。

ステップ S17-7 : コンテンツプロバイダ 101 は、ステップ S17-6 で圧縮したコンテンツデータを伸長してコンテンツデータを生成する。

ステップ S17-8 : コンテンツプロバイダ 101 は、伸長したコンテンツデータの聴覚検査を行う。

ステップ S17-9 : コンテンツプロバイダ 101 は、コンテンツデータに埋め込まれた電子透かし情報を、ステップ S17-5 でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。

そして、コンテンツプロバイダ 101 は、聴覚検査および電子透かし情報の検出の双方が成功した場合には、ステップ S17-10 の処理を行い、何れか一方が失敗した場合にはステップ S17-4 の処理を繰り返す。

【0090】

ステップ S17-10 : コンテンツプロバイダ 101 は、乱数を発生してコンテンツ鍵データ Kc を生成し、これを保持する。また、コンテンツプロバイダ 101 は、ステップ S17-6 で圧縮したコンテンツデータを、コンテンツ鍵データ Kc を用いて暗号化する。

【0091】

ステップ S17-11 : コンテンツプロバイダ 101 は、図 3 (A) に示すコンテンツファイル CF を作成し、これをコンテンツファイルデータベースに格納する。

【0092】

ステップS17-12:コンテンツプロバイダ101は、コンテンツデータCについての権利書データ106を作成する。

ステップS17-13:コンテンツプロバイダ101は、SRPを決定する。

ステップS17-14:コンテンツプロバイダ101は、コンテンツID、コンテンツ鍵データKcおよび権利書データ106をEMDサービスセンタ102に出力する。

ステップS17-15:コンテンツプロバイダ101は、ライセンス鍵データKD₁ ~ KD₃で暗号化されたキーファイルKFをEMDサービスセンタ102から入力する。

ステップS17-16:コンテンツプロバイダ101は、入力したキーファイルKFをキーファイルデータベースに格納する。

【0093】

ステップS17-17:コンテンツプロバイダ101は、コンテンツファイルCFとキーファイルKFとのリンク関係をハイパーリンクで結ぶ。

ステップS17-18:コンテンツプロバイダ101は、コンテンツファイルCFのハッシュ値をとり、秘密鍵データK_{CP,S}を用いて署名データSIG_{6,CP}を生成する。また、コンテンツプロバイダ101は、キーファイルKFのハッシュ値をとり、秘密鍵データK_{CP,S}を用いて署名データSIG_{7,CP}を生成する。

【0094】

ステップS17-19:コンテンツプロバイダ101は、図3に示すように、コンテンツファイルCF、キーファイルKF、公開鍵証明書データCER_{CP}、署名データSIG_{6,CP}、SIG_{7,CP}、SIG_{1,ESC}を格納したセキュアコンテナ104を作成する。

【0095】

ステップS17-20:複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップS17-1~B19の処理を繰り返して各々のセキュアコンテナ104を作成し、コンテンツファイルCFとキーファイルKFとの間のリンク関係と、コンテンツファイルCF相互間のリンク

関係とをハイパーリンクなどを用いて結ぶ。

ステップ S17-21: コンテンツプロバイダ 101 は、作成したセキュアコンテンツ 104 をセキュアコンテンツデータベースに格納する。

【0096】

[EMD サービスセンタ 102]

図 20 は、EMD サービスセンタ 102 の主な機能を示す図である。

EMD サービスセンタ 102 は、主に、図 20 に示すように、ライセンス鍵データをコンテンツプロバイダ 101 および $SAM105_1 \sim 105_4$ に供給する処理と、公開鍵証明書データ CER_{CP} , $CER_{SAM1} \sim CER_{SAM4}$ の発行処理と、キーファイル KF の発行処理、利用履歴データ 108 に基づいた決済処理（利益分配処理）とを行う。

【0097】

<ライセンス鍵データの供給処理>

まず、EMD サービスセンタ 102 からユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ にライセンス鍵データを送信する際の処理の流れを説明する。

EMD サービスセンタ 102 では、所定期間毎に、例えば、3 カ月分のライセンス鍵データ $KD_1 \sim KD_3$ を鍵データベースから読み出して、各々のハッシュ値をとり、EMD サービスセンタ 102 の秘密鍵データ $K_{ESC,S}$ を用いて、それぞれに対応する署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を作成する。

そして、EMD サービスセンタ 102 は、3 カ月分のライセンス鍵データ $KD_1 \sim KD_3$ およびそれらの署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を、 $SAM105_1 \sim 105_4$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、 $SAM105_1 \sim 105_4$ に送信する。

また、同様に、EMD サービスセンタ 102 は、コンテンツプロバイダ 101 に、例えば、6 カ月分のライセンス鍵データ $KD_1 \sim KD_6$ を送信する。

【0098】

<公開鍵証明書データの発行処理>

次に、EMD サービスセンタ 102 がコンテンツプロバイダ 101 から、公開

鍵証明書データ CER_{CP} の発行要求を受けた場合の処理を説明する。

EMDサービスセンタ 102 は、コンテンツプロバイダ 101 の識別子 CP_ID 、公開鍵データ $K_{CP,P}$ および署名データ $SIG_{9,CP}$ をコンテンツプロバイダ 101 から受信すると、これらを、コンテンツプロバイダ 101 との間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ $SIG_{9,CP}$ の正当性を検証した後に、識別子 CP_ID および公開鍵データ $K_{CP,P}$ に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ 101 が CP データベースに登録されているか否かを確認する。

そして、EMDサービスセンタ 102 は、当該コンテンツプロバイダ 101 の X. 509 形式の公開鍵証明書データ CER_{CP} を証明書データベースから読み出し、公開鍵証明書データ CER_{CP} のハッシュ値をとり、EMDサービスセンタ 102 の秘密鍵データ $K_{ESC,S}$ を用いて、署名データ $SIG_{1,ESC}$ を作成する。

そして、EMDサービスセンタ 102 は、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ を、コンテンツプロバイダ 101 との間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ 101 に送信する。

【0099】

なお、EMDサービスセンタ 102 が $SAM105_1$ から、公開鍵証明書データ CER_{SAM1} の発行要求を受けた場合の処理も、 $SAM105_1$ との間で処理が行われる点を除いて、公開鍵証明書データ CER_{CP} の発行要求を受けた場合の処理と同じである。公開鍵証明書データ CER_{CP} も、X. 509 形式で記述されている。

なお、本発明では、EMDサービスセンタ 102 は、例えば、 $SAM105_1$ の出荷時に、 $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ および公開鍵データ $K_{SAM1,P}$ を $SAM105_1$ の記憶部に記憶する場合には、当該出荷時に、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データ CER_{SAM1} を、 $SAM105_1$ の記憶部に記憶してもよい。

【0100】

＜キーファイルKFの発行処理＞

EMDサービスセンタ102は、コンテンツプロバイダ101から図6に示す登録用モジュールMod₂を受信すると、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK_{SES}を用いて登録用モジュールMod₂を復号する。

そして、EMDサービスセンタ102は、鍵データベースから読み出した公開鍵データK_{cp,p}を用いて、署名データSIG_{M1,CP}の正当性を検証する。

次に、EMDサービスセンタ102は、登録用モジュールMod₂に格納された権利書データ106、コンテンツ鍵データK_c、電子透かし情報管理データWMおよびSRPを、権利書データベースに登録する。

【0101】

次に、EMDサービスセンタ102は、鍵サーバから読み出した対応する期間のライセンス鍵データKD₁～KD₆を用いて、コンテンツ鍵データK_cおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃とを暗号化する。

次に、EMDサービスセンタ102は、ヘッダデータと、コンテンツ鍵データK_cおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃との全体に対してハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC,S}を用いて署名データSIG_{K1,ESC}を作成する。

次に、EMDサービスセンタ102は、図3(B)に示すキーファイルKFを作成し、これをKFデータベースに格納する。

次に、EMDサービスセンタ102は、KFデータベースにアクセスを行って得たキーファイルKFを、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0102】

＜決算処理＞

次に、EMDサービスセンタ102において行なう決済処理について説明する

EMDサービスセンタ102は、ユーザホームネットワーク103の例えばSAM105₁から利用履歴データ108およびその署名データSIG_{200,SAM1}を入力すると、利用履歴データ108および署名データSIG_{200,SAM1}を、SAM105₁との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM105₁の公開鍵データK_{SAM1}による署名データSIG_{200,SAM1}の検証を行う。

【0103】

図21は、利用履歴データ108に記述されるデータを説明するための図である。

図21に示すように、利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCに対してEMDサービスセンタ102によってグローバルユニークに付された識別子であるESC__コンテンツID、当該コンテンツデータCに対してコンテンツプロバイダ101によって付された識別子であるCP__コンテンツID、セキュアコンテナ104の配給を受けたユーザの識別子であるユーザID、当該ユーザのユーザ情報、セキュアコンテナ104の配給を受けたSAM105₁～105₄の識別子SAM__ID、当該SAMが属するホームネットワークグループの識別子であるHNG__ID、ディスカウント情報、トレーシング情報、プライスタグ、当該コンテンツデータを提供したコンテンツプロバイダ101の識別子CP__ID、紹介業者（ポータル:Portal）ID、ハードウェア提供者ID、セキュアコンテナ104を記録した記録媒体の識別子Media__ID、セキュアコンテナ104の提供に用いられた例えば圧縮方法などの所定のコンポーネントの識別子であるコンポーネントID、セキュアコンテナ104のライセンス所有者の識別子LH__ID、セキュアコンテナ104についての決済処理を行うEMDサービスセンタ102の識別子ESC__IDなどが記述されている。

なお、後述する第2実施形態では、利用履歴データ308には、上述した利用履歴データ108に記述されたデータに加えて、当該コンテンツデータCに対してサービスプロバイダ310によって付された識別子であるSP__コンテンツI

Dと、当該コンテンツデータCを配給したサービスプロバイダ310の識別子SP_IDとが記述されている。

【0104】

EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

【0105】

次に、EMDサービスセンタ102は、利用履歴データ108と、権利書データベースから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。

ここで、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

【0106】

次に、EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG₉₉を、相互認証およびセッション鍵データK_{SES}による復号を行った後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0107】

[ユーザホームネットワーク103]

ユーザホームネットワーク 103 は、図 1 に示すように、ネットワーク機器 160₁ および A/V 機器 160₂ ~ 160₄ を有している。

ネットワーク機器 160₁ は、SAM105₁ を内蔵している。また、A/V 機器 160₂ ~ 160₄ は、それぞれ SAM105₂ ~ 105₄ を内蔵している。

SAM105₁ ~ 105₄ の相互間は、例えば、IEEE1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。

なお、A/V 機器 160₂ ~ 160₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 160₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク 103 は、ネットワーク機能を有していない A/V 機器のみを有していてもよい。

【0108】

以下、ネットワーク機器 160₁ について説明する。

図 22 は、ネットワーク機器 160₁ の構成図である。

図 22 に示すように、ネットワーク機器 160₁ は、SAM105₁、通信モジュール 162、A/V 圧縮・伸長用 SAM163、操作部 165、ダウンロードメモリ 167、再生モジュール 169、外部メモリ 201 およびホスト CPU 810 を有する。

ここで、ホスト CPU 810 はネットワーク機器 160₁ 内の処理を統括的に制御しており、ホスト CPU 810 と SAM105₁ とは、それぞれマスタ (Master) とスレーブ (Slave) の関係にある。

以下、ホスト CPU 810 と SAM105₁ との関係を詳細に説明する。

図 23 は、ホスト CPU 810 と SAM105₁ との関係を説明するための図である。

図 23 に示すように、ネットワーク機器 160₁ では、ホスト CPU バス 1000 を介して、ホスト CPU 810 と SAM105₁ とが接続されている。

ホスト CPU 810 は、例えばユーザによる操作部 165 の操作に応じて複数の割り込みタイプの中から一の割り込みタイプが選択された場合に、当該選択さ

れた割り込みタイプを示す外部割り込み（ハードウェア割り込み）S165を受ける。

また、ホストCPU810は、外部割り込みS165を受け、当該外部割り込みS165に対応するタスクがSAM105₁が実行すべきものである場合に、当該タスクを指定した内部割り込み（ソフトウェア割り込み）S810を、ホストCPUバス1000を介してSAM105₁に出す。

【0109】

SAM105₁は、ホストCPU810からI/Oデバイスとして認識され、ホストCPU810からのファンクションコールである内部割り込みS810を受けて、要求に応じたタスクを実行し、当該タスクの実行結果をホストCPU810に返す。

SAM105₁が実行するタスクは、主に、コンテンツデータの購入処理（課金処理）、署名検証処理、相互認証処理、コンテンツデータの再生処理、更新処理、登録処理、ダウンロード処理などに関するものであり、これらのタスク群はSAM105₁内で外部から遮蔽された形で処理され、ホストCPU810は当該処理内容をモニタできない。

ホストCPU810は、どのようなイベントのときにSAM105₁にタスクを依頼するかを予め把握している。具体的には、ホストCPU810は、ユーザによる外部キーデバイスなどの操作部165の操作に応じた外部割り込みS165を受けて、当該割り込みによって実行すべきタスクがSAM105₁が実行するタスクであると判断すると、ホストCPUバス1000を介してSAM105₁に内部割り込みS810をかけ、SAM105₁に当該タスクを実行させる。

【0110】

ここで、コマンダーおよびキーボードなどの外部キーデバイスなどのホストCPU810に対してのI/Oデバイスに相当するものから受ける割り込みは、ホストCPU810が実行するユーザプログラムの内容とは全く非同期なイベントによって生じる割り込みであり、通常、これらを“ハードウェア割り込み”あるいは“外部割り込み”と呼んでいる。

ホストCPU810が、コンテンツの視聴および購入時に受ける割り込みは、

ハードウェア割り込みである。このとき、ハードウェア割り込みを発生する I / O デバイスは、例えば、ネットワーク機器 1 6 0₁ のボタン類や G U I (Graphic al User Interface) のアイコンなどのキーデバイスである。本実施形態では、これらの I / O デバイスを操作部 1 6 5 としている。

【0 1 1 1】

一方、ホスト CPU 8 1 0 によるユーザプログラム（プログラム）の実行に基づいて発生する割り込みは、“ソフトウェア割り込み”または”内部割り込み”と呼ばれる。

【0 1 1 2】

外部割り込み S 1 6 5 は、通常、その割り込み信号を、ホスト CPU バス 1 0 0 0 とは別に設けられた外部割り込み専用線を介して操作部 1 6 5 からホスト CPU 8 1 0 に出力している。

外部割り込み S 1 6 5 の種類は、割り込みが発生する I / O デバイスに番号を持たせることで区別される。例えば、キーボードなどでは、全てのボタン（当該番号を割り込みタイプと呼ぶ）に番号が割り当てられ、ボタンが押されると、当該ボタンが押下されたことを外部割り込み専用線を介して操作部 1 6 5 からホスト CPU 8 1 0 に通知し、当該押下されたボタンの番号を I / O インターフェイス内のメモリに記憶する。そして、ホスト CPU 8 1 0 は、ボタンが押下されたことの通知を受けると、I / O インターフェイス内のメモリにアクセスを行い、当該メモリに記憶されたボタンの番号から外部割り込みのタイプを識別し、当該ボタンの番号に対応する割り込みルーチンの実行制御を行う。

このとき、ホスト CPU 8 1 0 が、当該ボタンの番号に対応する割り込みルーチンが S A M 1 0 5₁ によって実行されるべきものである場合には、S A M 1 0 5₁ に内部割り込み S 8 1 0 を出してタスク実行を依頼する。

【0 1 1 3】

前述したように、S A M 1 0 5₁ が実行するタスクには、以下に示す①～③などがある。

これらのタスクは、外部割り込み専用線を介してホスト CPU 8 1 0 が①～③などに対応する外部割り込みを操作部 1 6 5 から受け、ホスト CPU 8 1 0 がそ

れに応じた内部割り込み S 8 1 0 を SAM 1 0 5₁ に出すことで、SAM 1 0 5₁ によって実行される。

①. コンテンツ購入処理（鍵の購入処理。試聴含む。）

②. 再生処理

③. コンテンツプロバイダ 1 0 1 および EMD サービスセンタ 1 0 2 からのダウンロード（更新処理、利用履歴回収、プログラムダウンロードなど）

【0114】

上記①、②では、割り込みを発生させる I/O はネットワーク機器 1 6 0₁ のボタンや GUI などの外部キーデバイスになる。

上記③は、実際は、コンテンツプロバイダ 1 0 1 からプッシュ的にダウンロード用のセキュアコンテナ 1 0 4 が送られてくるのではなく、ネットワーク機器 1 6 0₁（クライアント）側からポーリングしにいく能動的プル型のため、ダウンロードしたセキュアコンテナ 1 0 4 をネットワーク機器 1 6 0₁ 内のダウンロードメモリ 1 6 7 に書き込んだ時点で、その状態をホスト CPU 8 1 0 は把握している。従って、上記③の場合には、ホスト CPU 8 1 0 は、操作部 1 6 5 からの外部割り込み S 1 6 5 を受けることなく、SAM 1 0 5₁ に対して内部割り込み S 8 1 0 を発生する。

【0115】

SAM 1 0 5₁ は、ホスト CPU 8 1 0 に対してスレーブの I/O デバイスと機能するので、SAM 1 0 5₁ のメインルーチンは電源オンでスタートしてから、その後はスタンバイ（ウェーティング、待ち状態）モードで待機している。

その後、SAM 1 0 5₁ は、マスタであるホスト CPU 8 1 0 から内部割り込み S 8 1 0 を受けた時点で、内部で外部から遮蔽された形で依頼されたタスクを処理し、タスク終了をホスト CPU 8 1 0 に外部割り込み（ハードウェア割り込み）で知らせ、ホスト CPU 8 1 0 に当該そのタスク結果を拾ってもらう。従って、SAM 1 0 5₁ には、ユーザのメインプログラム（ユーザプログラム）というものがない。

【0116】

SAM 1 0 5₁ は、コンテンツの購入処理、再生処理、コンテンツプロバイダ

101、並びにEMDサービスセンタ102からのダウンロード処理などを割り込みルーチンとして実行する。SAM105₁は、通常は、スタンバイ状態で待機している状態から、ホストCPU810から内部割り込みS810を受け、その割り込みタイプ(番号)(ファンクションコールのコマンド)に応じた割り込みルーチンを実行し、結果を得た時点で、それをホストCPU810に拾ってもらう。

具体的には、ホストCPU810からSAM105₁への内部割り込みS810によるタスク依頼は、I/O命令で行われ、SAM105₁はホストCPU810から受け取ったファンクションコールのコマンドに基づいて自分自身に内部割り込みをかける。ホストCPU810によるSAM105₁への内部割り込みは、具体的には、チップセレクト(Chip Select)を行ってSAM105₁を選択して行われる。

【0117】

上述したように、コンテンツの購入および再生などの外部割り込みS165をホストCPU810が受けるにも係わらず、それに応じたタスクをSAM105₁に依頼して行うのは、それらのタスク内容が鍵の購入処理などに伴う暗号処理、署名生成、署名検証処理などのセキュリティに係わるものだからである。

SAM105₁に格納されている割り込みルーチンは、ホストCPU810のい割り込みルーチンのサブルーチン的な役割をもつ割り込みルーチンといえる。

ホストCPU810によって実行される割り込みルーチンは、SAM105₁の共有メモリ空間に、自らに対して行われた外部割り込みS165に対応するタスクを依頼する内部割り込み(ファンクションコール)S810を送ることを指示するタスクである。

なお、図24に示すように、SAM105₁に格納されている割り込みルーチンには、さらにサブルーチンがぶらさがっている。

他の割り込みルーチンに共通なプログラムは、サブルーチンとして定義したほうがコードサイズの節約になり、メモリの節減になるためである。また、SAM105₁の処理は、割り込みルーチンから並列にサブルーチンを定義したり、サブルーチンのさらにサブルーチンを定義するなど、通常のCPUの処理と同様の

手法が採用されている。

【0118】

図23に戻って説明を行う。

前述したように、ホストCPU810は、外部キーデバイスなどのI/Oからの割り込みを、割り込み専用線による外部割り込み（ハードウェア割り込み）S165として受ける。

各々の外部割り込み専用線には、番号が割り振られていて、その番号に応じてホストCPU810側のシステムメモリに格納されている割り込みベクタテーブルにおいて、相当の割り込みベクタを抜き出して割り込みルーチンを開始する。そのとき、割り込みタイプが、ベクタテーブルの中の割り込みベクタの選択番号を示す間接アクセスと、割り込みタイプが、そのまま割り込みルーチンの開始アドレスを示す直接アクセスの2種類が存在する。

【0119】

ホストCPU810は、受けた外部割り込みが、SAM105₁が行うべきタスクの場合、割り込みルーチンは、SAM105₁に対して内部割り込みS810をかけ、SAM105₁にタスクを実行するように依頼（I/O命令）するプログラムである。

タスクの種類はコマンド名で定義されていて、ホストCPU810はSAM105₁に対してコマンドベースの内部割り込みS810をかける。SAM105₁は電源オンしたとき、図24に示すように、初期化プログラムとSAM内部のIntegrity Checkを済ませ、その後はスタンバイ状態で待機するスリープモードとなる。スリープモードでは、CPUの動作のみを停止させ、すべての割り込みで復帰する。その後、SAM105₁は、例外処理状態を経てプログラム実行状態に遷移する。その後は、SAM105₁は、ホストCPU810からのタスク依頼の内部割り込みを受けた時点で相当のタスクを実行して結果を出し、それをホストCPU810に返す。

ホストCPU810は、その結果を受けて次のアクションを行う。但し、SAM105₁がタスク実行中でも、ホストCPU810は他のタスクを行ってもよい。ホストCPU810は、SAM105₁によるタスクの実行結果を割り込み

として受けつける。

【0120】

SAM105₁ が、ホストCPU810から依頼を受けたタスクの実行結果をホストCPU810に知らせる手段としては、ホストCPU810に対し割り込みをかけて、ホストCPU810に当該実行結果を拾ってもらう方法と、SAM105₁ の内部のホストCPU810がアクセス可能なアドレス空間上（当該アドレス空間には、ホストCPU810からのリード／ライトコマンド、アドレス情報、データがキャリーされる）にステータスレジスタ（SAMステータスレジスタと呼ぶ）を設ける方法とがある。後者の方法では、SAMステータスレジスタ（SAM__SR）にタスクの種類、タスク待機中、タスク実行中、タスク終了などのフラグを設定できるようにし、当該SAMステータスレジスタに、ホストCPU810から定期的にポーリング（データの読み込み）を行う。

【0121】

第1のSAMステータスレジスタには、ホストCPU810によって読み出される、SAM105₁ のステータス（状態）を示すフラグが設定される。

また、第2のSAMステータスレジスタには、ホストCPU810からタスク実行の依頼が出されているか否かのステータスをSAM105₁ の内部のCPUから読みに行くフラグが設定される。バス調停の優先順位に基づいて、ホストCPU810とSAM105₁ との双方が、当該第1および第2のSAMステータスレジスタのフラグにアクセスできる。

【0122】

具体的には、第1のSAMステータスレジスタには、現在SAMがタスクを実行中か否か、タスク終了済で結果が得られているか否か、そのときのタスク名は何か、あるいはSAMは現在スタンバイ中でタスク待ちの状態か否かを示すフラグが設けられている。第1のSAMステータスレジスタには、ホストCPU810が定期的にポーリングしに行く。

一方、第2のSAMステータスレジスタには、ホストCPU810からタスク実行の依頼が発生しているか否か、あるいは待機中か否かを示すフラグが設けられている。

ここで、ホストCPU 810からは、I/O書き込み命令のコマンドがI/OデバイスであるSAM105₁に送られ、続いて、書き込むデータと書き込むアドレス情報が送られる。そのときのアドレス情報（データの格納場所）はホストCPU 810とSAM105₁との共有メモリ空間内に格納される。

【0123】

ここで、SAM105₁内のメモリのアドレス空間は、ホストCPU 810側からは見えなくすることが必要なので（耐タンパ性）、ホストCPU 810からは、作業スタック用のSRAMの一部、あるいは外付けのFlash-ROM（EEPROM）の一部しか見えなくように、SAM105₁内のアドレス空間を管理する回路を構成する。従って、ホストCPU 810から、データ量の大きいものは、これらのエリアにデータを書き込んでいくし、データ量の少ないものはSAM105₁の内部に、ホストCPU 810から見えるように仮設のレジスタを設定して、そこに書き込む。

【0124】

割り込みによって実行される割り込みルーチンのアドレスは「割り込みベクタ」と呼ばれる。割り込みベクタは、割り込みタイプの順に割り込みベクタテーブルに格納されている。

【0125】

ホストCPU 810は、図25に示すように、外部割り込みを受けると、その割り込みタイプ（番号）にしたがって、メモリに格納された割り込みベクタテーブルから割り込みベクタを取り出し、そのアドレスから始まるルーチンをサブルーチンとして実行する。

本実施形態では、前述した①～③の場合に、対応するI/Oから物理的な割り込み信号によって外部割り込みが発生し、その割り込みタイプ（番号）にしたがって実行される割り込みルーチンで、I/OであるSAM105₁に対して内部割り込み（ソフトウェア割り込み）を利用したファンクションコール（Procedure Call）を行い、自分の代わりにSAM105₁にそのタスクの実行を行ってもらい、その結果を受け取って次なるアクションを行う。

内部割り込みは、図26に示すように、ユーザプログラム中、つまりCPU内

部から発生するソフトウェア割り込みである。当該内部割り込みは、マシン語の INT 命令の実行によって発生する。

【0 1 2 6】

以下、ファンクションコール (Procedure Call) について説明する。

割り込みルーチンの中は、さらに細かく機能 (ファンクション) に分けられていて、各機能にコマンド名が定義されている。ここで、ユーザプログラムから、割り込み命令 INT と共にコマンドを指定することで、目的の機能を指定することをファンクションコール (Procedure Call) とよぶ。ファンクションコールは、内部割り込み (ソフトウェア割り込み) を利用したものである。

ファンクションコールでは、CPU のレジスタにファンクションコール番号を入れて割り込みルーチンに必要なパラメータを渡し、目的の機能 (ファンクション) を指定する。その結果はレジスタやメモリに返されるか、あるいは動作となつてあらわれる。

例えば、ホスト CPU 8 1 0 が図 2 7 に示すユーザプログラム内のコード A を実行する場合には、「INT 2 1 H」によって CPU によって割り込みタイプ「2 1 H」の内部割り込みに対応するメモリ内の領域がアクセスされ、コマンド解析部へのアクセスを介して、ファンクション 3 のサブルーチンが実行される。

【0 1 2 7】

次に、SAM 1 0 5₁ の CPU の処理状態について説明する。

図 2 8 は、SAM 1 0 5₁ の CPU の処理状態を説明するための図である。

図 2 8 に示すように、SAM 1 0 5₁ の CPU の処理状態には、リセット状態 ST 1、例外処理状態 ST 2、バス権解放状態 ST 3、プログラム実行状態 ST 4 および低消費電力状態 ST 5 の 5 種類がある。

以下、各状態について説明する。

リセット状態 ST 1 : CPU がリセットされている状態である。

例外処理状態 ST 2 : リセットや割り込みなどの例外処理要因によって CPU が処理状態の流れを変えるときに過渡的な状態である。割り込みの処理の場合は、SP (スタックポインタ) を参照して PC (プログラムカウンタ) のカウント値とステータスレジスタ (SR) の値とをスタック領域に退避する。例外処理ベ

クターテーブルから割り込みルーチンの開始アドレスを取り出し、そのアドレスに分岐してプログラムの実行を開始する。その後の処理状態はプログラム実行状態 S T 3 となる。

【 0 1 2 8 】

プログラム実行状態 S T 3 : C P U が順次プログラムを実行している状態である。

バス権解放状態 S T 4 : C P U がバス権を要求したデバイスにバスを解放する状態である。

【 0 1 2 9 】

低消費電力状態 S T 5 : スリープモード、スタンバイモードおよびモジュールスタンバイモードの 3 つの状態がある。

(1) スリープモード

C P U の動作は停止するが、C P U の内部レジスタのデータと、内蔵キャッシュメモリ、および内蔵 R A M のデータは保持される。C P U 以外の内蔵周辺モジュールの機能は停止しない。

このモードからの復帰は、リセット、すべての割り込み、または D M A アドレスエラーによって行われ、例外処理状態 S T 2 を経て通常のプログラム実行状態へ遷移する。

(2) スタンバイモード

スタンバイモードでは、C P U 、内蔵モジュール、および発振器のすべての機能が停止する。

キャッシュおよび内部 R A M のデータは保持されない。

スタンバイモードからの復帰は、リセット、外部の N M I 割り込みにより行われる。

復帰時は、発振安定時間経過後、例外処理状態を経て通常プログラム状態へ遷移する。

発振器が停止するので、消費電力は著しく低下する。

(3) モジュールスタンバイモード

D M A などの内蔵モジュールへのクロック供給を停止することができる。

【0130】

次に、ホストCPU810とSAM105₁ との関係メモリ空間を用いて説明する。

図29は、ホストCPU810およびSAM105₁ のメモリ空間を示す図である。

図29に示すように、ホストCPU810のCPU810aは、ユーザのボタン操作などに応じた外部割り込みを受けると、ユーザプログラムの実行を中断して、割り込みタイプを指定して割り込みベクタテーブルのハードウェア割り込みの領域にアクセスする。そして、CPU810aは、当該アクセスによって得られたアドレスに記憶されている割り込みルーチンを実行する。当該割り込みルーチンは、SAMに対して内部割り込みであるファンクションコールCall1-1, 1-2, 2または3を出してSAMに対応するタスクを実行させ、そのタスク実行の結果を得た後に、ユーザプログラムに復帰する処理を記述している。具体的には、CPU810aは、SAM105₁ 内のメモリ105₁ aの一部を構成するSRAM1155に、依頼するタスクを特定する情報を書き込む。ここで、SRAM1155は、ホストCPU810とSAM105₁ との共有メモリである。

【0131】

ホストCPU810のCPU810aは、SAM105₁ に内部割り込みを出すときに、SAM105₁ 内の第2のSAMステータスレジスタ1156bのタスク待機中のフラグをオンにする。

SAM105₁ のCPU1100は、第2のSAMステータスレジスタ1156bを見ると、SRAM1155にアクセスして依頼されたタスクの種類を特定し、それに応じた割り込みルーチンを実行する。当該割り込みルーチンは、前述したように、他のサブルーチンを読み出して実行される。当該サブルーチンには、例えば、記録媒体との相互認証、A/V圧縮・伸長用SAMとの相互認証、メディア・ドライブSAMとの間の相互認証、ICカードとの間の相互認証、機器間の相互認証、EMDサービスセンタ102との間の相互認証、並びに署名データの生成および検証を行うものがある。

【0132】

SAM105₁ のCPU1100は、当該割り込みルーチンの結果（タスク結果）を、SRAM1155内に格納すると共に、SAM105₁ 内の第1のSAMステータスレジスタ1156aのタスク終了のフラグをオンにする。

そして、ホストCPU810は、第1のSAMステータスレジスタ1156aのタスク終了のフラグがオンにされたことを確認した後に、SRAM1155に格納されたタスク結果を読み出し、その後、ユーザプログラムの処理に復帰する。

【0133】

以下、SAM105₁ の機能を説明する。

ここで、SAM105₂ ~ 105₄ の機能は、SAM105₁ の機能と同じである。

SAM105₁ は、コンテンツ単位の課金処理を行うモジュールであり、EMDサービスセンタ102との間で通信を行う。

SAM105₁ は、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁ のIC(Integrated Circuit)の内部の仕様を知ることはできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネットワーク機器160₁ に搭載される。なお、SAM105₂ ~ 105₄ は、それぞれAV機器160₂ ~ 160₄ に搭載される。

【0134】

SAM105₁ は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistance)性を持ったハードウェアモジュール(ICモジュールなど)、あるいはCPUにおいてソフトウェア(秘密プログラム)を実行して実現される機能モジュールである。

SAM105₁ の機能を IC という形で実現する場合は、IC 内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMを IC という物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分を SAM として定義してもよい。

【0135】

なお、図 22 に示す例では、実線で示されるように、通信モジュール 162 からのセキュアコンテナ 104 を SAM105₁ に出力する場合を例示するが、点線で示されるように、通信モジュール 162 から SAM105₁ にキーファイル KF を出力し、通信モジュール 162 からダウンロードメモリ 167 に CPU バスなどを介してコンテンツファイル CF を直接的にダウンロードメモリ 167 に書き込むようにしてもよい。

また、AV 圧縮・伸長用 SAM163 に対してのコンテンツデータ C の出力は、SAM105₁ を介して行うのではなく、ダウンロードメモリ 167 から直接的に行うようにしてもよい。

【0136】

以下、SAM105₁ の機能を機能ブロック図を参照しながら具体的に説明する。

図 30 は、SAM105₁ の機能の機能ブロック図である。

なお、図 30 には、コンテンツプロバイダ 101 からのセキュアコンテナ 104 を入力し、セキュアコンテナ 104 内のキーファイル KF を復号する処理に関連するデータの流れが示されている。

図 30 に示すように、SAM105₁ は、相互認証部 170、暗号化・復号部 171、172、173、コンテンツプロバイダ管理部 180、ダウンロードメモリ管理部 182、AV 圧縮・伸長用 SAM 管理部 184、EMD サービスセンタ管理部 185、利用監視部 186、課金処理部 187、署名処理部 189、SAM 管理部 190、メディア SAM 管理部 197、作業用メモリ 200、外部メモリ管理部 811 および CPU1100 を有する。

CPU1100 は、ホスト CPU810 からの内部割り込み S810 を受けて、SAM105₁ 内の処理を統括的に制御する。

【0 1 3 7】

ここで、コンテンツプロバイダ管理部 1 8 0 およびダウンロードメモリ管理部 1 8 2 が本発明の入力処理手段に対応し、課金処理部 1 8 7 が本発明の決定手段、履歴データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部 1 7 2 が本発明の復号手段に対応し、利用監視部 1 8 6 が本発明の利用制御手段に対応している。

また、暗号化・復号部 1 7 3 が本発明の暗号化手段に対応している。

また、後述する例えば図 4 5 に示すメディア・ドライブ SAM 管理部 8 5 5 が本発明の記録制御手段に対応している。

また、署名処理部 1 8 9 が本発明の署名処理手段に対応している。

【0 1 3 8】

なお、図 3 0 に示す SAM 1 0 5₁ の各機能は、前述したように、CPU において秘密プログラムを実行して実現されるか、あるいは所定のハードウェアによって実現される。SAM 1 0 5₁ のハードウェア構成については後述する。

また、外部メモリ 2 0 1 には、以下に示す処理を経て、図 3 1 に示すように、利用履歴データ 1 0 8 および SAM 登録リストが記憶される。

ここで、外部メモリ 2 0 1 のメモリ空間は、SAM 1 0 5₁ の外部（例えば、ホスト CPU 8 1 0）からは見ることはできず、SAM 1 0 5₁ のみが外部メモリ 2 0 1 の記憶領域に対してのアクセスを管理できる。

外部メモリ 2 0 1 としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。

また、作業用メモリ 2 0 0 としては、例えば SRAM が用いられ、図 3 2 に示すように、セキュアコンテナ 1 0 4、コンテンツ鍵データ K_c、権利書データ（UCP）1 0 6、記憶部 1 9 2 のロック鍵データ K_{L0C}、コンテンツプロバイダ 1 0 1 の公開鍵証明書 CER_{CP}、利用制御データ（UCS）1 6 6、および SAM プログラム・ダウンロード・コンテナ SDC₁ ~ SDC₃ などが記憶される。

【0 1 3 9】

以下、SAM 1 0 5₁ の機能のうち、コンテンツプロバイダ 1 0 1 からのセキュアコンテナ 1 0 4 を入力（ダウンロード）したときの各機能ブロックの処理内

容を図 30 を参照しながら説明する。

当該処理は、コンテンツのダウンロードを指示する外部割り込み S810 をホスト CPU810 から受けた CPU1100 によって統括的に制御される。

【0140】

相互認証部 170 は、SAM105₁ がコンテンツプロバイダ 101 および EMD サービスセンタ 102 との間でオンラインでデータを送受信する際に、コンテンツプロバイダ 101 および EMD サービスセンタ 102 との間で相互認証を行ってセッション鍵データ（共有鍵） K_{SES} を生成し、これを暗号化・復号部 171 に出力する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0141】

暗号化・復号部 171 は、コンテンツプロバイダ 101 および EMD サービスセンタ 102 との間で送受信するデータを、相互認証部 170 が生成したセッション鍵データ K_{SES} を用いて暗号化・復号する。

【0142】

ダウンロードメモリ管理部 182 は、図 22 に示すようにダウンロードメモリ 167 が相互認証機能を持つメディア SAM167a を有している場合には、相互認証部 170 とメディア SAM167a との間で相互認証を行った後に、相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化して図 22 に示すダウンロードメモリ 167 に書き込む。

ダウンロードメモリ 167 としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図 33 に示すように、HDD (Hard Disk Drive) などの相互認証機能を備えていないメモリをダウンロードメモリ 211 として用いる場合には、ダウンロードメモリ 211 内はセキュアではないので、コンテンツファイル CF をダウンロードメモリ 211 にダウンロードし、機密性の高いキーファイル KF を例えば、図 30 に示す作業用メモリ 200 あるいは図 22 に示す外部メモリ 201 にダウンロードする。

キーファイル KF を外部メモリ 201 に記憶する場合には、例えば、SAM1

05₁において、キーファイルKFをCBCモードでMAC鍵データK_{MAC}を用いて暗号化して外部メモリ201に記憶し、最後の暗号文ブロックの一部をMAC (Message Authentication Code) 値としSAM105₁内に記憶する。そして、外部メモリ201からSAM105₁にキーファイルKFを読み出す場合には、SAM105₁内で当該読み出したキーファイルKFをMAC鍵データK_{MAC}を用いて復号し、それによって得たMAC値と、既に記憶しているMAC値とを比較することで、キーファイルKFが改竄されているか否かを検証する。この場合に、MAC値ではなく、ハッシュ値を用いてもよい。

【0143】

暗号化・復号部172は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKF内のコンテンツ鍵データK_c、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を、記憶部192から読み出した対応する期間のライセンス鍵データKD₁～KD₃を用いて復号する。

当該復号されたコンテンツ鍵データK_c、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃は、作業用メモリ200に書き込まれる。

【0144】

EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

【0145】

署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データK_{ESC,P}およびコンテンツプロバイダ101の公開鍵データK_{CP,P}を用いて、セキュアコンテナ104内の署名データの検証を行なう。

【0146】

記憶部192は、SAM105₁の外部から読み出しおよび書き換えできない秘密データとして、図34に示すように、有効期限付きの複数のライセンス鍵データKD₁～KD₃、SAM__ID、ユーザID、パスワード、当該SAMが属するホームネットワークグループの識別子HNG__ID、情報参照用ID、SA

M登録リスト、機器および記録媒体のリボケーションリスト、記録用鍵データ K_{STR} 、ルートCAの公開鍵データ $K_{R-CA,P}$ 、EMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ 、EMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ 、ドライブ用SAMの認証用元鍵（共通鍵暗号化方式を採用した場合）、ドライブ用SAMの公開鍵証明書（秘密鍵暗号化方式を採用した場合）、 $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ （共通鍵暗号化方式を採用した場合）、 $SAM105_1$ の公開鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書 CER_{SAM1} （秘密鍵暗号化方式を採用した場合）、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いた公開鍵証明書 CER_{ESC} の署名データ SIG_{22} 、AV圧縮・伸長用SAM163との間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAMとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAMの公開鍵証明書データ CER_{MEDSAM} （公開鍵暗号化方式を採用した場合）、扱える信号の諸元、圧縮方式、接続するモニタ表示能力、フォーマット変換機能、ビットストリームレコーダの有無、権利処理（利益分配）用データ、利益分配する関連エンティティのIDなどを記憶している。

なお、図34において、左側に「*」を付したデータは、 $SAM105_1$ の出荷時に記憶部192に記憶されており、それ以外のデータは出荷後に行われるユーザー登録時に記憶部192に記憶される。

【0147】

また、記憶部192には、図30に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部192としては、例えば、フラッシューEEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0148】

<ライセンス鍵データの受信時の処理>

以下、EMDサービスセンタ102から受信したライセンス鍵データ $KD_1 \sim KD_3$ を記憶部192に格納する際の $SAM105_1$ 内での処理の流れを図33および図35を参照しながら説明する。

図35は、EMDサービスセンタ102から受信したライセンス鍵データ KD

$1 \sim KD_3$ を記憶部 192 に格納する際の SAM105₁ 内での処理の流れを示すフローチャートである。

ステップ S35-0 : SAM105₁ の CPU1100 は、ホスト CPU810 から、ライセンス鍵データの受信処理を行うことを指示する内部割り込み S810 を受ける。

ステップ S35-1 : SAM105₁ の相互認証部 170 と、EMD サービスセンタ 102 との間で相互認証を行なう。

ステップ S35-2 : ステップ S35-1 の相互認証によって得られたセッション鍵データ K_{SES} で暗号化した 3 カ月分のライセンス鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を、EMD サービスセンタ 102 から EMD サービスセンタ管理部 185 を介して作業用メモリ 200 に書き込む。

【0149】

ステップ S35-3 : 暗号化・復号部 171 は、セッション鍵データ K_{SES} を用いて、ライセンス鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を復号する。

ステップ S35-4 : 署名処理部 189 は、作業用メモリ 200 に記憶された署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ の正当性を確認した後に、ライセンス鍵データ $KD_1 \sim KD_3$ を記憶部 192 に書き込む。

ステップ S35-5 : CPU1100 は、上述したライセンス鍵データ受信処理が適切に行われたか否かを、外部割り込みでホスト CPU810 に通知する。

なお、CPU1100 は、上述したライセンス鍵データ受信処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU810 がポーリングによって当該フラグを読んでもよい。

【0150】

<セキュアコンテナ 104 をコンテンツプロバイダ 101 から入力した時の処理>

以下、コンテンツプロバイダ 101 が提供したセキュアコンテナ 104 を入力する際の SAM105₁ 内での処理の流れを図 30 および図 36 を参照しながら

説明する。

なお、以下に示す例では、コンテンツファイルCFをSAM105₁を介してダウンロードメモリ167に書き込む場合を例示するが、本発明は、コンテンツファイルCFをSAM105₁を介さずに直接的にダウンロードメモリ167に書き込むようにしてもよい。

図36は、コンテンツプロバイダ101が提供したセキュアコンテナ104を入力する際のSAM105₁内での処理の流れを示すフローチャートである。

なお、以下に示す例では、SAM105₁において、セキュアコンテナ104を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ104の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップS36-0：図30に示すSAM105₁のCPU1100は、ホストCPU810から、セキュアコンテナの入力処理を行うことを指示する内部割り込みS810を受ける。

ステップS36-1：SAM105₁の相互認証部170とコンテンツプロバイダ101との間で相互認証を行なう。

ステップS36-2：SAM105₁の相互認証部170とダウンロードメモリ167のメディアSAM167aとの間で相互認証を行なう。

【0151】

ステップS36-3：コンテンツプロバイダ101から受信したセキュアコンテナ104を、ダウンロードメモリ167に書き込む。

このとき、ステップS36-2で得られたセッション鍵データを用いて、相互認証部170におけるセキュアコンテナ104の暗号化と、メディアSAM167aにおけるセキュアコンテナ104の復号とを行なう。

ステップS36-4：SAM105₁は、ステップS36-1で得られたセッション鍵データを用いて、セキュアコンテナ104の復号を行なう。

【0152】

ステップS36-5：署名処理部189は、図3(C)に示す署名データSIG_{1,ESC}の検証を行なった後に、図3(C)に示す公開鍵証明書データCER_{CP}

内に格納されたコンテンツプロバイダ 101 の公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{6,CP}$ 、 $SIG_{7,CP}$ の正当性を検証する。

このとき、署名データ $SIG_{6,CP}$ が正当であると検証されたときに、コンテンツファイル CF の作成者および送信者の正当性が確認される。

また、署名データ $SIG_{7,CP}$ が正当であると検証されたときに、キーファイル KF の送信者の正当性が確認される。

【0153】

ステップ S36-6：署名処理部 189 は、記憶部 192 から読み出した公開鍵データ $K_{ESC,P}$ を用いて、図 3（B）に示すキーファイル KF 内の署名データ $SIG_{K1,ESC}$ の正当性、すなわちキーファイル KF の作成者の正当性およびキーファイル KF が EMD サービスセンタ 102 に登録されているか否かの検証を行う。

【0154】

ステップ S36-7：暗号化・復号部 172 は、記憶部 192 から読み出した対応する期間のライセンス鍵データ $KD_1 \sim KD_3$ を用いて、図 3（B）に示すキーファイル KF 内のコンテンツ鍵データ Kc 、権利書データ 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ を復号し、これらを作業用メモリ 200 に書き込む。

【0155】

ステップ S36-8：CPU 1100 は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホスト CPU 810 に通知する。

なお、CPU 1100 は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU 810 がポーリングによって当該フラグを読んでもよい。

【0156】

以下、ダウンロードメモリ 167 にダウンロードされたコンテンツデータ C を利用・購入する処理に関連する各機能ブロックの処理内容を図 37 を参照しながら説明する。

以下に示す各機能ブロックの処理は、ホスト CPU 810 からの内部割り込み

S810を受けたCPU1100によって統括的に制御される。

【0157】

利用監視部186は、作業用メモリ200から権利書データ106および利用制御データ166を読み出し、当該読み出した権利書データ106および利用制御データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ106は、図36を用いて説明したように、復号後に作業用メモリ200に記憶されたキーファイルKF内に格納されている。

また、利用制御データ166は、後述するように、ユーザによって購入形態が決定されたときに、作業用メモリ200に記憶される。

なお、利用制御データ166には、当該コンテンツデータCを購入したユーザのユーザIDおよびトレーシング(Tracing)情報が記述され、取扱制御情報として購入形態決定処理で決定された購入形態が記述されている点を除いて、図3に示す権利書データ106と同じデータが記述されている。

【0158】

課金処理部187は、図22に示すホストCPU810からコンテンツの購入あるいは利用の形態を決定することを指示する内部割り込みS810を受けたときに、それに応じた利用履歴データ108を作成する。

ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0159】

また、課金処理部187は、必要に応じて、作業用メモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。

ここで、販売価格および標準小売価格データSRPは、復号後に作業用メモリ200に記憶された図3(B)に示すキーファイルKFの権利書データ106内に格納されている。

課金処理部187による課金処理は、利用監視部186の監視の下、権利書デ

ータ 106 が示す使用許諾条件などの権利内容および利用制御データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0160】

また、課金処理部 187 は、外部割り込み S810 に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御 (UCS: Usage Control Status) データ 166 を生成し、これを作業用メモリ 200 に書き込む。

本実施形態では、購入形態を決定した後に、利用制御データ 166 を作業用メモリ 200 に記憶する場合を例示したが、利用制御データ 166 およびコンテンツ鍵データ Kc を外付けメモリである外部メモリ 201 に格納するようにしてもよい。外部メモリ 201 としは、前述したように、例えば NVRAM であるフラッシュメモリが用いられる。外部メモリ 201 に書き込みを行う場合には外部メモリ 201 の正当性の検証であるインテグリティチェック (Integrity Check) を行うが、この際に外部メモリ 201 の記憶領域を複数のブロックに分け、ブロック毎に SHA-1 あるいは MAC などでハッシュ値を求め、当該ハッシュ値を SAM105₁ 内で管理する。

なお、SAM105₁ において、購入形態を決定せずに、セキュアコンテナ 104 を他の SAM105₂ ~ 105₄ に転送してもよい。この場合には、利用制御データ 166 は作成されない。

【0161】

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切り (Sell Through)、利用期間に制限を持たせるタイムリミテッド (Time Limited)、再生する度に課金を行なう再生課金 (Pay Per Play)、SCMS 機器を用いた複製において再生する度に課金を行なう再生課金 (Pay Per SCMS)、SCMS 機器において複製を認める (Sell Through SCMS Copy)、および複製のガードを行わずに再生する度に課金を行う再生課金 (Pay Per Copy N without copy guard) などがある。

ここで、利用制御データ 166 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが

当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ 166 には、コンテンツの ID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれた SAM の SAM_ID、購入を行なったユーザの USER_ID などが記述されている。

【0162】

なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁ からコンテンツプロバイダ 101 に利用制御データ 166 をコンテンツデータ C の購入と同時にリアルタイムに送信し、コンテンツプロバイダ 101 が EMD サービスセンタ 102 に、利用履歴データ 108 を所定の期間内に SAM105₁ に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御データ 166 が、コンテンツプロバイダ 101 および EMD サービスセンタ 102 の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御データ 166 をコンテンツプロバイダ 101 にリアルタイムに送信する。

【0163】

EMD サービスセンタ管理部 185 は、所定の期間毎に、外部メモリ管理部 811 を介して外部メモリ 201 から読み出した利用履歴データ 108 を EMD サービスセンタ 102 に送信する。

このとき、EMD サービスセンタ管理部 185 は、署名処理部 189 において、秘密鍵データ $K_{SAM1,s}$ を用いて利用履歴データ 108 の署名データ $SIG_{200,SAM1}$ を作成し、署名データ $SIG_{200,SAM1}$ を利用履歴データ 108 と共に EMD サービスセンタ 102 に送信する。

EMD サービスセンタ 102 への利用履歴データ 108 の送信は、例えば、EMD サービスセンタ 102 からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ 108 に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ 201 の記憶容量に応じて決定される。

【0164】

ダウンロードメモリ管理部182は、例えば、図22に示すホストCPU810からコンテンツの再生動作を行う旨の内部割り込みS810をCPU1100が受けた場合に、ダウンロードメモリ167から読み出したコンテンツデータC、作業用メモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196をAV圧縮・伸長用SAM管理部184に出力する。

また、AV圧縮・伸長用SAM管理部184は、ホストCPU810からの外部割り込みS165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びに作業用メモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199をAV圧縮・伸長用SAM管理部184に出力する。

【0165】

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。AV圧縮・伸長用SAM163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、AV圧縮・伸長用SAM163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【0166】

＜ダウンロードしたセキュアコンテナの購入形態決定処理＞

以下、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでのSAM105₁の処理の流れを図37および図38を参照しながら説明する。

なお、以下に示す処理では、セキュアコンテナ104の購入形態を決定する際に、セキュアコンテナ104内の各データの署名データの検証を行わない（前述

したようにセキュアコンテナ 104 の受信時に署名データの検証を行う) 場合を例示するが、当該購入形態を決定する際にこれらの署名データの検証を行ってもよい。

図 38 は、コンテンツプロバイダ 101 からダウンロードメモリ 167 にダウンロードされたセキュアコンテナ 104 の購入形態を決定するまでの処理の流れを示すフローチャートである。

ステップ S38-0: 図 37 に示す SAM105₁ の CPU1100 は、ホスト CPU810 から、コンテンツの購入形態を決定することを指示する内部割り込み S810 を受ける。

【0167】

ステップ S38-1: CPU1100 は、ホスト CPU810 からの内部割り込み S810 が試聴モードを指定しているか否かを判断し、指定されたと判断した場合にはステップ S38-2 の処理を実行し、出力されていないと判断した場合にはステップ S38-5 の処理を実行する。

【0168】

ステップ S38-2: 作業用メモリ 200 から読み出されたコンテンツ鍵データ K_c および半開示パラメータデータ 199 が、図 32 に示す AV 圧縮・伸長用 SAM163 に出力される。このとき、相互認証部 170 と相互認証部 220 との間の相互認証後に、コンテンツ鍵データ K_c および半開示パラメータデータ 199 に対してセッション鍵データ K_{SES} による暗号化および復号が行なわれる。

【0169】

ステップ S38-3: CPU1100 は、ホスト CPU810 から試聴モードを行うことを示す内部割り込み S810 を受けると、例えば、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が、AV 圧縮・伸長用 SAM 管理部 184 を介して、図 22 に示す AV 圧縮・伸長用 SAM163 に出力される。

このとき、コンテンツファイル CF に対して、相互認証部 170 とメディア SAM167a との間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号と、相互認証部 170 と相互認証部 220 との間の相互認証およびセッショ

ン鍵データ K_{SES} による暗号化・復号とが行なわれる。

コンテンツファイル CF は、図 2 2 に示す AV 圧縮・伸長用 $SAM163$ の復号部 2 2 1 においてセッション鍵データ K_{SES} を用いて復号された後に、復号部 2 2 2 に出力される。

【0 1 7 0】

ステップ $S38-4$: 復号された半開示パラメータデータ 1 9 9 が半開示処理部 2 2 5 に出力され、半開示処理部 2 2 5 からの制御によって、復号部 2 2 2 によるコンテンツ鍵データ K_c を用いたコンテンツデータ C の復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータ C が、伸長部 2 2 3 において伸長された後に、電子透かし情報処理部 2 2 4 に出力される。

次に、電子透かし情報処理部 2 2 4 においてコンテンツデータ C にユーザ電子透かし情報用データ 1 9 6 が埋め込まれ、コンテンツデータ C が再生モジュール 1 6 9 において再生され、コンテンツデータ C に応じた音響が出力される。

また、電子透かし情報処理部 2 2 4 では、コンテンツデータ C に埋め込まれている電子透かし情報が検出され、当該検出の結果に基づいて、処理の停止の有無を決定する。

【0 1 7 1】

ステップ $S38-5$: ユーザが操作部 1 6 5 を操作して購入形態を決定すると、当該決定に応じた内部割り込み $S810$ がホスト $CPU810$ から $SAM105_1$ に出される。

ステップ $S38-6$: $SAM105_1$ の課金処理部 1 8 7 において、決定された購入形態に応じた利用履歴データ 1 0 8 および利用制御データ 1 6 6 が生成され、利用履歴データ 1 0 8 が外部メモリ管理部 8 1 1 を介して外部メモリ 2 0 1 に書き込まれると共に、利用制御データ 1 6 6 が作業用メモリ 2 0 0 に書き込まれる。

以後は、利用監視部 1 8 6 において、利用制御データ 1 6 6 によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【0 1 7 2】

ステップ S 3 8－7：後述する図 3 9（C）に示す新たなキーファイル $K F_1$ が作成され、当該作成されたキーファイル $K F_1$ がダウンロードメモリ管理部 1 8 2 を介してダウンロードメモリ 1 6 7 あるいはその他のメモリに記憶される。

図 3 9（C）に示すように、キーファイル $K F_1$ に格納された利用制御データ 1 6 6 はストレージ鍵データ K_{STR} およびメディア鍵データ K_{MED} を用いて DES の CBC モードを利用して順に暗号化されている。

ここで、記録用鍵データ K_{STR} は、例えば SACD (Super Audio Compact Disc)、DVD (Digital Versatile Disc) 機器、CD-R 機器および MD (Mini Disc) 機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを 1 対 1 で対応づけるために用いられる。また、メディア鍵データ K_{MED} は、記録媒体にユニークなデータである。

【0 1 7 3】

ステップ S 3 8－8：署名処理部 1 8 9 において、 $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ を用いて、キーファイル $K F_1$ のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイル $K F_1$ と対応付けられて作業用メモリ 2 0 0 に書き込まれる。ハッシュ値 H_{K1} は、キーファイル $K F_1$ の作成者の正当性およびキーファイル $K F_1$ が改竄されたか否かを検証するために用いられる。

なお、購入形態が決定されたコンテンツデータ C を、例えば、記録媒体に記録したり、オンラインを介して送信する場合には、図 3 9 に示すように、キーファイル $K F_1$ およびハッシュ値 H_{K1} 、コンテンツファイル C F およびその署名データ $SIG_{6,CP}$ 、キーファイル K F およびその署名データ $SIG_{7,CP}$ 、公開鍵証明書データ CER_{cp} およびその署名データ $SIG_{1,ESC}$ 、公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ を格納したセキュアコンテナ 1 0 4 p が作成される。

上述したようにセキュアコンテナ 1 0 4 の購入形態を決定すると、利用制御データ 1 6 6 が生成されて作業用メモリ 2 0 0 に記憶されるが、 $SAM105_1$ において再び同じセキュアコンテナ 1 0 4 について購入形態を再決定する場合には

、操作信号 S 1 6 5 に応じて作業用メモリ 2 0 0 に記憶されている利用制御データ 1 6 6 が更新される。

【0174】

ステップ S 3 8-9 : CPU 1 1 0 0 は、上述したコンテンツの購入形態決定処理が適切に行われたか否かを、外部割り込みでホスト CPU 8 1 0 に通知する。

なお、CPU 1 1 0 0 は、上述したコンテンツの購入形態決定処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU 8 1 0 がポーリングによって当該フラグを読んでもよい。

【0175】

＜コンテンツデータの再生処理＞

次に、ダウンロードメモリ 1 6 7 に記憶されている購入形態が既に決定されたコンテンツデータ C を再生する場合の処理の流れを、図 4 0 を参照しながら説明する。

図 4 0 は、当該処理を示すフローチャートである。

当該処理を行う前提として、前述した購入形態の決定処理によって作業用メモリ 2 0 0 に、利用制御データ 1 6 6 が格納されている。

ステップ S 4 0-0 : 図 3 7 に示す SAM 1 0 5₁ の CPU 1 1 0 0 は、ホスト CPU 8 1 0 から、コンテンツの再生処理を行うことを指示する内部割り込み S 8 1 0 を受ける。

【0176】

ステップ S 4 0-1 : 作業用メモリ 2 0 0 から利用監視部 1 8 6 に、利用制御データ 1 6 6 が読み出され、利用制御データ 1 6 6 が示す再生条件が解釈・検証され、その結果に基づいて以後の再生処理が行われるように監視される。

ステップ S 4 0-2 : 図 3 7 に示す相互認証部 1 7 0 と、図 2 2 に示す AV 圧縮・伸長用 SAM 1 6 3 の相互認証部 2 2 0 との間で相互に認証が行われ、セッション鍵データ K_{SES} が共有される。

【0177】

ステップ S 4 0-3 : ステップ S 4 0-1 で解釈・検証された再生条件と、作

業用メモリ 2 0 0 から読み出されたコンテンツ鍵データ K_c とが、ステップ S 4 0 - 2 で得られたセッション鍵データ K_{SES} を用いて暗号化された後に、A V 圧縮・伸長用 S A M 1 6 3 に出力される。

これによって、図 2 2 に示す A V 圧縮・伸長用 S A M 1 6 3 の復号部 2 2 1 においてセッション鍵データ K_{SES} を用いて再生条件およびコンテンツ鍵データ K_c が復号される。

【 0 1 7 8 】

ステップ S 4 0 - 4 : ダウンロードメモリ 1 6 7 から読み出されたコンテンツファイル C F が、ステップ S 4 0 - 2 で得られたセッション鍵データ K_{SES} を用いて暗号化された後に、A V 圧縮・伸長用 S A M 1 6 3 に出力される。

これによって、図 2 2 に示す A V 圧縮・伸長用 S A M 1 6 3 の復号部 2 2 1 においてセッション鍵データ K_{SES} を用いてコンテンツファイル C F が復号される。続いて、A V 圧縮・伸長用 S A M 1 6 3 の伸長部 2 2 3 において、コンテンツファイル C F 内のコンテンツデータ C が伸長され、電子透かし情報処理部 2 2 4 においてユーザ電子透かし情報を埋め込んだ後に再生モジュール 1 6 9 において再生される。

【 0 1 7 9 】

ステップ S 4 0 - 5 : 必要に応じて、ステップ S 4 0 - 1 で読み出された利用制御データ 1 6 6 が更新され、再び作業用メモリ 2 0 0 に書き込まれる。

また、外部メモリ 2 0 1 に記憶されている利用履歴データ 1 0 8 が更新あるいは作成される。

【 0 1 8 0 】

ステップ S 4 0 - 6 : C P U 1 1 0 0 は、上述したコンテンツの再生処理が適切に行われたか否かを、外部割り込みでホスト C P U 8 1 0 に通知する。

なお、C P U 1 1 0 0 は、上述したコンテンツの再生処理が適切に行われたか否かを示す S A M ステータスレジスタのフラグを設定し、ホスト C P U 8 1 0 がポーリングによって当該フラグを読んでもよい。

【 0 1 8 1 】

<一の機器の利用制御データ (U S C) 1 6 6 を使用して他の機器で再購入を

行う場合の処理＞

先ず、図 4 1 に示すように、例えば、ネットワーク機器 160₁ のダウンロードメモリ 167 にダウンロードされたコンテンツファイル CF の購入形態を前述したように決定した後に、当該コンテンツファイル CF を格納した新たなセキュアコンテナ 104 x を生成し、バス 191 を介して、AV 機器 160₂ の SAM 105₂ にセキュアコンテナ 104 x を転送するまでの SAM 105₁ 内での処理の流れを図 4 2 および図 4 3 を参照しながら説明する。

【0182】

図 4 3 は、当該処理のフローチャートである。

図 4 3 に示す処理を行う前提として、前述した購入処理によって、SAM 105₁ の作業用メモリ 200 には図 4 4 (C) に示すキーファイル KF₁ およびハッシュ値 H_{K1} が記憶されている。

ステップ S 4 3 - 1 : ユーザによる操作部 165 の操作に応じて、購入形態を既に決定したセキュアコンテナを SAM 105₂ に転送することを示す内部割り込み S 8 1 0 を、図 4 2 に示す CPU 1100 が受ける。

それに応じて、課金処理部 187 は、外部メモリ 201 に記憶されている利用履歴データ 108 を更新する。

【0183】

ステップ S 4 3 - 2 : SAM 105₁ は、後述する SAM 登録リストを検証し、セキュアコンテナの転送先の SAM 105₂ が正規に登録されている SAM であるか否かを検証し、正規に登録されていると判断した場合にステップ S 4 3 - 3 以降の処理を行う。

また、SAM 105₁ は、SAM 105₂ がホームネットワーク内の SAM であるか否かの検証も行う。

【0184】

ステップ S 4 3 - 3 : 相互認証部 170 は、SAM 105₂ との間で相互認証を行って得たセッション鍵データ K_{SES} を共用する。

【0185】

ステップ S 4 3 - 4 : SAM 管理部 190 は、ダウンロードメモリ 211 から

図 39 (A) に示すコンテンツファイル CF および署名データ $SIG_{6,CP}$ を読み出し、これについての $SAM105_1$ の秘密鍵データ K_{SAM1} を用いた署名データ $SIG_{41,SAM1}$ を署名処理部 189 に作成させる。

【0186】

ステップ S43-5 : SAM 管理部 190 は、ダウンロードメモリ 211 から図 39 (B) に示すキーファイル KF および署名データ $SIG_{7,CP}$ を読み出し、これについての $SAM105_1$ の秘密鍵データ K_{SAM1} を用いた署名データ $SIG_{42,SAM1}$ を署名処理部 189 に作成させる。

【0187】

ステップ S43-6 : SAM 管理部 190 は、図 44 に示すセキュアコンテナ 104x を作成する。

ステップ S43-7 : 暗号化・復号部 171 において、ステップ S43-3 で得たセッション鍵データ K_{SES} を用いて、図 44 に示すセキュアコンテナ 104x が暗号化される。

【0188】

ステップ S43-8 : SAM 管理部 190 は、セキュアコンテナ 104x を図 41 に示す AV 機器 160₂ の $SAM105_2$ に出力する。

このとき、 $SAM105_1$ と $SAM105_2$ との間の相互認証と並行して、IEEE 1394 シリアルバスであるバス 191 の相互認証が行われる。

【0189】

ステップ S43-9 : CPU 1100 は、上述した購入形態を既に決定したセキュアコンテナを $SAM105_2$ に転送する処理が適切に行われたか否かを、外部割り込みでホスト CPU 810 に通知する。

なお、CPU 1100 は、上述した購入形態を既に決定したセキュアコンテナを $SAM105_2$ に転送する処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU 810 がポーリングによって当該フラグを読んでもよい。

【0190】

以下、図 41 に示すように、 $SAM105_1$ から入力した図 44 に示すセキュ

アコンテナ 1 0 4 x を、RAM 型などの記録媒体（メディア）1 3 0₄ に書き込む際の SAM 1 0 5₂ 内での処理の流れを図 4 5、図 4 6 および図 4 7 を参照して説明する。

図 4 6 および図 4 7 は、当該処理を示すフローチャートである。

ここで、RAM 型の記録媒体 1 3 0₄ は、例えば、セキュアでない RAM 領域 1 3 4、メディア SAM 1 3 3 およびセキュア RAM 領域 1 3 2 を有している。

ステップ S 4 6 - 0 : 図 4 5 に示す CPU 1 1 0 0 は、図 4 1 に示す AV 機器 1 6 0₂ のホスト CPU 8 1 0 から、ネットワーク機器 1 6 0₁ からのセキュアコンテナを入力することを示す内部割り込み S 8 1 0 を受ける。

【0 1 9 1】

ステップ S 4 6 - 1 : SAM 1 0 5₂ は、SAM 登録リストを検証し、セキュアコンテナの転送元の SAM 1 0 5₁ が正規に登録されている SAM であるか否かを検証し、正規に登録されていると判断した場合にステップ S 4 6 - 2 以降の処理を行う。

また、SAM 1 0 5₂ は、SAM 1 0 5₁ がホームネットワーク内の SAM であるか否かの検証も行う。

【0 1 9 2】

ステップ S 4 6 - 2 : 前述したステップ S 4 3 - 2 に対応する処理として、SAM 1 0 5₂ は、SAM 1 0 5₁ との間で相互認証を行って得たセッション鍵データ K_{SES} を共用する。

ステップ S 4 6 - 3 : SAM 1 0 5₂ の SAM 管理部 1 9 0 は、図 4 1 および図 4 5 に示すように、ネットワーク機器 1 6 0₁ の SAM 1 0 5₁ からセキュアコンテナ 1 0 4 x を入力する。

ステップ S 4 6 - 4 : 暗号化・復号部 1 7 1 は、ステップ S 4 6 - 2 で共用したセッション鍵データ K_{SES} を用いて、SAM 管理部 1 9 0 を介して入力したセキュアコンテナ 1 0 4 x を復号する。

【0 1 9 3】

ステップ S 4 6 - 5 : セッション鍵データ K_{SES} を用いて復号されたセキュアコンテナ 1 0 4 x 内のコンテンツファイル CF が、図 3 9 に示すメディア・ドラ

ブSAM260におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体130₄のRAM領域134に記録される。

【0194】

ステップS46-6:セッション鍵データ K_{SES} を用いて復号されたセキュアコンテナ104x内の署名データ $SIG_{6,CP}$ 、 $SIG_{41,SAM1}$ と、キーファイルKFおよびその署名データ $SIG_{7,CP}$ 、 $SIG_{42,SAM1}$ と、キーファイル KF_1 およびそのハッシュ値 H_{K1} と、公開鍵署名データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とが、作業用メモリ200に書き込まれる。

【0195】

ステップS46-7:署名処理部189において、記憶部192から読み出した公開鍵データ $K_{CP,P}$ を用いて、公開鍵証明書データ CER_{CP} 、 CER_{SAM1} の正当性が確認される。

そして、署名処理部189において、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{6,CP}$ の正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。また、署名処理部189において、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{SAM1,P}$ を用いて、署名データ $SIG_{41,SAM1}$ の正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。

【0196】

ステップS46-8:署名処理部189は、公開鍵データ K_{CP} 、 $K_{SAM1,P}$ を用いて、作業用メモリ200に記憶されている署名データ $SIG_{7,CP}$ 、 $SIG_{42,SAM1}$ の正当性を検証する。そして、署名データ $SIG_{7,CP}$ 、 $SIG_{42,SAM1}$ が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0197】

ステップS46-9:署名処理部189は、記憶部192から読み出した公開鍵データ $K_{ESC,P}$ を用いて、図44(B)に示すキーファイルKFに格納された

署名データ $SIG_{K1,ESC}$ の正当性を確認する。

そして、署名データ $SIG_{K1,ESC}$ が正当であると検証されたときに、キーファイル KF の作成者の正当性が確認される。

【0198】

ステップ $S46-10$: 署名処理部 189 は、ハッシュ値 H_{K1} の正当性を検証し、キーファイル KF_1 の作成者および送信者の正当性を確認する。

なお、当該例では、キーファイル KF_1 の作成者と送信元とが同じ場合を述べたが、キーファイル KF_1 の作成者と送信元とが異なる場合には、キーファイル KF_1 に対して作成者の署名データと送信者と署名データとが作成され、署名処理部 189 において、双方の署名データの正当性が検証される。

【0199】

ステップ $S46-11$: 利用監視部 186 は、ステップ $S46-10$ で復号されたキーファイル KF_1 に格納された利用制御データ 166 を用いて、以後のコンテンツデータ C の購入・利用形態を制御する。

【0200】

ステップ $S46-12$: ユーザが操作部 165 を操作して購入形態を決定すると、それに応じた内部割り込み $S810$ を $SAM105_2$ の $CPU1100$ が受ける。

ステップ $S46-13$: 課金処理部 187 は、 $CPU1100$ からの制御に基づいて、外部メモリ 201 に記憶されている利用履歴データ 108 を更新する。

また、課金処理部 187 は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ 166 を更新する。

このとき送信元の SAM の利用制御データ 166 は破棄される。

【0201】

ステップ $S46-14$: 暗号化・復号部 173 は、記憶部 192 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を順に用いて、ステップ $S46-12$ で生成された利用制御データ 166 を暗号化してメディア・ドライブ SAM 管理部 855 に出力する。

ステップ $S46-15$: メディア・ドライブ SAM 管理部 855 は、新たな利

用制御データ 1 6 6 を格納したキーファイル $K F_1$ を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体 $1 3 0_4$ のセキュアRAM領域 1 3 2 に記録する。

なお、メディア鍵データ K_{MED} は、図 4 5 に示す相互認証部 1 7 0 と図 4 1 に示すRAM型の記録媒体 $1 3 0_4$ のメディアSAM 1 3 3 との間の相互認証によって記憶部 1 9 2 に事前に記憶されている。

【0 2 0 2】

ここで、記録用鍵データ K_{STR} は、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類(当該例では、AV機器 $1 6 0_2$)に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとでは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データ K_{STR} は、このような場合において、不正コピーを防止する役割を果たす。

なお、本実施形態では、記録用鍵データ K_{STR} を用いた暗号化を行わないようにしてもよい。

【0 2 0 3】

また、メディア鍵データ K_{MED} は、記録媒体(当該例では、RAM型の記録媒体 $1 3 0_4$)にユニークなデータである。

メディア鍵データ K_{MED} は、記録媒体(当該例では、図 4 1 に示すRAM型の記録媒体 $1 3 0_4$)側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データ K_{MED} を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データ K_{MED} は、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内の図示しないホストCPUの管理外の領域に記憶されている。

なお、本実施形態のように、機器側のSAM(当該例では、SAM 1 0 5₂)

とメディアSAM（当該例では、メディアSAM133）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データ K_{MED} を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データ K_{MED} を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データ K_{STR} およびメディア鍵データ K_{MED} が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0204】

また、購入者鍵データ K_{PIN} は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データ K_{PIN} は、EMDサービスセンタ102において管理される。

【0205】

ステップS46-16：キーファイルKFが作業用メモリ200から読み出され、メディア・ドライブSAM管理部855を介して、図41に示すメディア・ドライブSAM260によってRAM型の記録媒体130₄のセキュアRAM領域132に書き込まれる。

【0206】

ステップS46-17：SAM105₂のCPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。

なお、CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0207】

また、上述した実施形態では、メディア・ドライブSAM260による処理を経て、キーファイルKF、 KF_1 をRAM型の記録媒体130₄のセキュアRAM領域132に記録する場合を例示したが、図41において点線で示すように、SAM105₂からメディアSAM133にキーファイルKF、 KF_1 を記録するようにしてもよい。

【0208】

また、上述した実施形態では、SAM105₁ からSAM105₂ にセキュアコンテナ104xを送信する場合を例示したが、ネットワーク機器160₁ のホストCPUおよびAV機器160₂ のホストCPUによって、コンテンツファイルCFおよび権利書データ106をネットワーク機器160₁ からAV機器160₂ に送信してもよい。この場合には、SAM105₁ からSAM105₂ に、利用制御データ166およびコンテンツ鍵データKcが送信される。

【0209】

また、その他の実施形態として、例えば、SAM105₁ において購入形態を決定し、SAM105₂ では購入形態を決定せずに、SAM105₁ において生成した利用制御データ166をSAM105₂ でそのまま用いてもよい。この場合には、利用履歴データ108は、SAM105₁ において生成され、SAM105₂ では生成されない。

また、コンテンツデータCの購入は、例えば、複数のコンテンツデータCからなるアルバムを購入する形態で行ってもよい。この場合に、アルバムを構成する複数のコンテンツデータCは、異なるコンテンツプロバイダ101によって提供されてもよい（後述する第2実施形態の場合には、さらに異なるサービスプロバイダ310によって提供されてもよい）。また、アルバムを構成する一部のコンテンツデータCについての購入を行った後に、その他のコンテンツデータCを追加する形で購入を行い、最終的にアルバムを構成する全てのコンテンツデータCを購入してもよい。

【0210】

図48は、コンテンツデータCの種々の購入形態の例を説明するための図である。

図48に示すように、AV機器160₃ は、ネットワーク機器160₁ がコンテンツプロバイダ101から受信したコンテンツデータCを、権利書データ106を用いて購入し、利用制御データ166aを生成している。

また、AV機器160₂ は、ネットワーク機器160₁ がコンテンツプロバイダ101から受信したコンテンツデータCを、権利書データ106を用いて購入

し、利用制御データ 166b を生成している。

また、AV機器 160₃ は、AV機器 160₂ が購入したコンテンツデータ C を複製し、AV機器 160₂ で作成した利用制御データ 166b を用いて利用形態を決定している。これにより、AV機器 160₃ において、利用制御データ 166c が作成される。また、AV機器 160₃ では、利用制御データ 166c から利用履歴データ 108b が作成される。

また、AV機器 160₄ は、ネットワーク機器 160₁ がコンテンツプロバイダ 101 から受信して購入形態を決定したコンテンツデータ C を入力し、ネットワーク機器 160₁ が作成した利用制御データ 166 を用いて当該コンテンツデータ C の購入形態を決定する。これにより、AV機器 160₄ において、利用制御データ 166a が作成される。また、AV機器 160₄ では、利用制御データ 166a から利用履歴データ 108a が作成される。

なお、利用制御データ 166a, 166b, 166c は、AV機器 160₄, 160₂, 160₃ において、それぞれ固有の記録用鍵データ S_{STR}、並びに記録メディア（媒体）に固有のメディア鍵データ K_{MED} を用いて暗号化され、記録媒体に記録される。

本実施形態では、ユーザは、コンテンツデータ C の所有権に対して対価を支払うのではなく、使用权に対価を支払う。コンテンツデータの複製は、コンテンツのプロモーションに相当し、マーケットの拡販という観点からコンテンツデータの権利者の要請にかなう行為となる。

【0211】

＜ROM型の記録媒体のコンテンツデータの購入形態決定処理＞

図 49 に示すように、コンテンツの購入形態が未決定の図 11 に示す ROM 型の記録媒体 130₁ をユーザホームネットワーク 303 がオフラインで配給を受けた場合に、AV機器 160₂ において購入形態を決定する際の処理の流れを図 50 および図 51 を参照しながら説明する。

図 51 は、当該処理のフローチャートである。

ステップ S51-0：ユーザによる操作部 165 の操作に応じて、ROM 型の記録媒体を用いて配給されたコンテンツの購入形態を決定することを示す内部割り

込み S 8 1 0 を、図 5 0 に示す SAM 1 0 5₂ の CPU 1 1 0 0 が受ける。

ステップ S 5 1 - 1 : SAM 1 0 5₂ は、図 5 0 に示す相互認証部 1 7 0 と図 1 1 に示す ROM 型の記録媒体 1 3 0₁ のメディア SAM 1 3 3 との間で相互認証を行った後に、メディア SAM 1 3 3 からメディア鍵データ K_{MED} を入力する。

なお、SAM 1 0 5₂ が、事前にメディア鍵データ K_{MED} を保持している場合には、当該入力を行わなくても良い。

【 0 2 1 2 】

ステップ S 5 1 - 2 : ROM 型の記録媒体 1 3 0₁ のセキュア RAM 領域 1 3 2 に記録されているセキュアコンテナ 1 0 4 に格納された図 3 (B) , (C) に示すキーファイル K F およびその署名データ S I G_{7,CP} と、公開鍵証明書データ C E R_{CP} およびその署名データ S I G_{1,ESC} とを、メディア・ドライブ SAM 管理部 8 5 5 を介して入力して作業用メモリ 2 0 0 に書き込む。

【 0 2 1 3 】

ステップ S 5 1 - 3 : 署名処理部 1 8 9 において、署名データ S I G_{1,ESC} の正当性を確認した後に、公開鍵証明書データ C E R_{CP} から公開鍵データ K_{CP,P} を取り出し、この公開鍵データ K_{CP,P} を用いて、署名データ S I G_{7,CP} の正当性、すなわちキーファイル K F の送信者の正当性を検証する。

また、署名処理部 1 8 9 において、記憶部 1 9 2 から読み出した公開鍵データ K_{ESC,P} を用いて、キーファイル K F に格納された署名データ S I G_{K1,ESC} の正当性、すなわちキーファイル K F の作成者の正当性を検証する。

【 0 2 1 4 】

ステップ S 5 1 - 4 : 署名処理部 1 8 9 において署名データ S I G_{7,CP} , S I G_{K1,ESC} の正当性が確認されると、作業用メモリ 2 0 0 から暗号化・復号部 1 7 2 にキーファイル K F を読み出す。

次に、暗号化・復号部 1 7 2 において、対応する期間のライセンス鍵データ K D₁ ~ K D₃ を用いて、キーファイル K F に格納されたコンテンツ鍵データ K c 、権利書データ 1 0 6 および SAM プログラム・ダウンロード・コンテナ S D C₁ ~ S D C₃ を復号した後に、作業用メモリ 2 0 0 に書き込む。

【0215】

ステップS51-5：図50に示す相互認証部170と図49に示すAV圧縮・伸長用SAM163との間で相互認証を行った後に、SAM105₂のAV圧縮・伸長用SAM管理部184は、作業用メモリ200に記憶されているコンテンツ鍵データK_cおよび権利書データ106に格納された半開示パラメータデータ199、並びにROM型の記録媒体130₁のROM領域131から読み出したコンテンツファイルCFに格納されたコンテンツデータCを図49に示すAV圧縮・伸長用SAM163に出力する。

次に、AV圧縮・伸長用SAM163において、コンテンツデータCがコンテンツ鍵データK_cを用いて半開示モードで復号された後に伸長され、再生モジュール270に出力される。そして、再生モジュール270において、AV圧縮・伸長用SAM163からのコンテンツデータCが再生される。

【0216】

ステップS51-6：ユーザによる図49に示す操作部165の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す内部割り込みS810が、SAM1052のCPU1100に出される。

【0217】

ステップS51-7：課金処理部187は、操作信号S165に応じた利用制御データ166を作成し、これを作業用メモリ200に書き込む。

ステップS51-8：作業用メモリ200から暗号化・復号部173に、コンテンツ鍵データK_cおよび利用制御データ166が出力される。

暗号化・復号部173は、作業用メモリ200から入力したコンテンツ鍵データK_cおよび利用制御データ166を、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化して作業用メモリ200に書き込む。

【0218】

ステップS51-9：メディアSAM管理部197において、作業用メモリ200から読み出した、暗号化されたコンテンツ鍵データK_cおよび利用制御データ166と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を

用いて図44 (C) に示すキーファイル KF_1 が生成される。

また、署名処理部189において、図44 (C) に示すキーファイル KF_1 のハッシュ値 H_{K1} が生成され、当該ハッシュ値 H_{K1} がメディア・ドライブSAM管理部855に出力される。

図50に示す相互認証部170と図49に示すメディアSAM133との間で相互認証を行った後に、メディア・ドライブSAM管理部855は、キーファイル KF_1 およびハッシュ値 H_{K1} を、図49に示すメディア・ドライブSAM260を介してROM型の記録媒体130₁ のセキュアRAM領域132に書き込む。

これにより、購入形態が決定されたROM型の記録媒体130₁ が得られる。

このとき、課金処理部187が生成した利用制御データ166および利用履歴データ108は、所定のタイミングで、作業用メモリ200および外部メモリ201からそれぞれ読み出しされたEMDサービスセンタ102に送信される。

なお、ROM型の記録媒体130₁ のメディアSAM133にキーファイル KF が格納されている場合には、図49において点線で示されるように、SAM105₂ はメディアSAM133からキーファイル KF を入力する。また、この場合に、SAM105₂ は、作成したキーファイル KF_1 をメディアSAM133に書き込む。

【0219】

ステップS51-10：SAM105₂ のCPU1100は、上述したROM型の記録媒体を用いて配給されたコンテンツの購入形態を決定する処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。

なお、CPU1100は、上述したROM型の記録媒体を用いて配給されたコンテンツの購入形態を決定する処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0220】

<ROM型の記録媒体のコンテンツデータの購入形態を決定した後に、RAM型の記録媒体に書き込む場合の処理>

以下、図52に示すように、AV機器160₃ において購入形態が未決定のR

ROM型の記録媒体 130₁ からセキュアコンテナ 104 を読み出して新たなセキュアコンテナ 104_y を生成し、これを AV 機器 160₂ に転送し、AV 機器 160₂ において購入形態を決定して RAM 型の記録媒体 130₅ に書き込む際の処理の流れを図 53、図 54、図 55 を参照しながら説明する。

なお、ROM 型の記録媒体 130₁ から RAM 型の記録媒体 130₅ へのセキュアコンテナ 104_y の転送は、図 1 に示すネットワーク機器 160₁ および AV 機器 160₁ ~ 160₄ のいずれの間で行ってもよい。

図 55 は、当該処理のフローチャートである。

【0221】

ステップ S55-0 : ユーザによる操作部 165 の操作に応じて、購入形態が未決定の ROM 型の記録媒体から読み出したセキュアコンテナを SAM105₂ に転送することを示す内部割り込み S810 を、図 53 に示す CPU1100 が受ける。

ステップ S55-1 : SAM105₃ は、SAM 登録リストを検証し、セキュアコンテナの転送先の SAM105₂ が正規に登録されている SAM であるか否かを検証し、正規に登録されていると判断した場合にステップ S55-2 以降の処理を行う。

また、SAM105₃ は、SAM105₂ がホームネットワーク内の SAM であるか否かの検証も行う。

ステップ S55-2 : SAM105₃ と SAM105₂ との間で相互認証が行われ、セッション鍵データ K_{SES} が共有される。

【0222】

ステップ S55-3 : AV 機器 160₃ の SAM105₃ と ROM 型の記録媒体 130₁ のメディア SAM133 との間で相互認証を行い、ROM 型の記録媒体 130₁ のメディア鍵データ K_{MED1} を SAM105₃ に転送する。

なお、メディア鍵データ K_{MED1} を用いた暗号化を ROM 型の記録媒体 130₁ のメディア SAM133 において行う場合には、メディア鍵データ K_{MED1} の転送は行わない。

【0223】

ステップ S55-4 : AV 機器 160₂ の SAM105₂ と RAM 型の記録媒体 130₅ のメディア SAM133 との間で相互認証を行い、RAM 型の記録媒体 130₅ のメディア鍵データ K_{MED2} を SAM105₂ に転送する。

なお、メディア鍵データ K_{MED2} を用いた暗号化を RAM 型の記録媒体 130₅ のメディア SAM133 において行う場合には、メディア鍵データ K_{MED2} の転送は行わない。

【0224】

ステップ S55-5 : SAM105₃ は、図 53 に示すように、メディア・ドライブ SAM 管理部 855 を介して、ROM 型の記録媒体 130₁ の ROM 領域 131 からコンテンツファイル CF およびその署名データ $SIG_{6,CP}$ を読み出し、これを SAM 管理部 190 に出力すると共に、署名処理部 189 において、秘密鍵データ $K_{SAM3,S}$ を用いて、これらの署名データ $SIG_{350,SAM3}$ を作成する。

【0225】

ステップ S55-6 : SAM105₃ は、図 53 に示すように、メディア・ドライブ SAM 管理部 855 を介して、ROM 型の記録媒体 130₁ のセキュア RAM 領域 132 からキーファイル KF およびその署名データ $SIG_{7,CP}$ を読み出し、これを SAM 管理部 190 に出力すると共に、署名処理部 189 において、秘密鍵データ $K_{SAM3,S}$ を用いて、これらの署名データ $SIG_{352,SAM3}$ が作成される。

【0226】

ステップ S55-7 : SAM105₃ において、記憶部 192 から SAM 管理部 190 に公開鍵証明書データ CER_{SAM3} およびその署名データ $SIG_{351,ESC}$ が読み出される。

【0227】

ステップ S55-8 : SAM105₃ の例えば SAM 管理部 190 において、図 54 に示すセキュアコンテナ 104_y が作成される。

【0228】

ステップ S55-9 : SAM105₃ の暗号化・復号部 171 において、ステ

ステップ S55-2 で得たセッション鍵データ K_{SES} を用いて、セキュアコンテナ 104y が暗号化される。

【0229】

ステップ S55-10 : SAM105₃ の SAM 管理部 190 から AV 機器 160₂ に、セキュアコンテナ 104y が出力される。

そして、SAM105₃ の CPU1100 から ホスト CPU810 に、外部割り込みで、上述した処理が適切に行われたか否かが通知される。

なお、CPU1100 は、上述した処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU810 がポーリングによって当該フラグを読んでもよい。

SAM105₂ では、ホスト CPU810 からの内部割り込み S810 による CPU1100 の制御によって、図 57 に示すように、SAM 管理部 190 を介して SAM105₃ から入力した図 54 に示すセキュアコンテナ 104y が暗号化・復号部 171 においてセッション鍵データ K_{SES} を用いて復号される。

そして、当該復号されたセキュアコンテナ 104y 内のキーファイル KF およびその署名データ $SIG_{7,CP}$ 、 $SIG_{350,SAM3}$ と、公開鍵証明書データ CER_{SAM3} およびその署名データ $SIG_{351,ESC}$ と、公開鍵証明書データ CER_{cp} およびその署名データ $SIG_{1,ESC}$ とが、作業用メモリ 200 に書き込まれる。

【0230】

ステップ S55-12 : SAM105₂ の署名処理部 189 において、セキュアコンテナ 104y 内に格納された署名データ $SIG_{6,CP}$ 、 $SIG_{350,SAM3}$ の正当性、すなわちコンテンツファイル CF の作成者および送信者の正当性を確認する。

ステップ S55-13 : コンテンツファイル CF の作成者および送信者が正当であると確認された後に、メディア・ドライブ SAM 管理部 855 を介して RAM 型の記録媒体 130₅ の RAM 領域 134 にコンテンツファイル CF が書き込まれる。

なお、コンテンツファイル CF は、ホスト CPU810 の制御によって、SAM を介さずに、RAM 型の記録媒体 130₅ の RAM 領域 134 に直接的に記録

してもよい。

【 0 2 3 1 】

ステップ S 5 5 - 1 4 : 署名処理部 1 8 9 において、署名データ $S I G_{351, EC_S}$ が署名検証され、公開鍵証明書データ $C E R_{S A M 3}$ の正当性が確認された後に、公開鍵証明書データ $C E R_{S A M 3}$ に格納された公開鍵データ $K_{S A M 3}$ および公開鍵データ $K_{E S C, P}$ を用いて、署名データ $S I G_{7, C P}$ 、 $S I G_{352, S A M 3}$ 、 $S I G_{K 1, E S C}$ の正当性、すなわちキーファイル $K F$ の作成者および送信者の正当性が確認される。

【 0 2 3 2 】

ステップ S 5 5 - 1 5 : キーファイル $K F$ の作成者および送信者の正当性が確認されると、作業用メモリ 2 0 0 からキーファイル $K F$ が読み出されて暗号化・復号部 1 7 2 に出力され、暗号化・復号部 1 7 2 において、ライセンス鍵データ $K D_1 \sim K D_3$ を用いて復号された後に、作業用メモリ 2 0 0 に書き戻される。

【 0 2 3 3 】

ステップ S 5 5 - 1 6 : 作業用メモリ 2 0 0 に記憶されている既に復号されたキーファイル $K F$ に格納された権利書データ 1 0 6 が、利用監視部 1 8 6 に出力される。そして、利用監視部 1 8 6 において、権利書データ 1 0 6 に基づいて、コンテンツの購入形態および利用形態が管理（監視）される。

【 0 2 3 4 】

ステップ S 5 5 - 1 7 : ユーザによる図 5 2 に示す操作部 1 6 5 の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた内部割り込み S 8 1 0 が、ホスト CPU 8 1 0 から $S A M 1 0 5_2$ の CPU 1 1 0 0 に出される。

ステップ S 5 5 - 1 8 : 課金処理部 1 8 7 において、決定された購入・利用形態に応じて利用制御データ 1 6 6 および利用履歴データ 1 0 8 が生成され、これが作業用メモリ 2 0 0 および外部メモリ 2 0 1 にそれぞれ書き込まれる。

利用制御データ 1 6 6 および利用履歴データ 1 0 8 は、所定のタイミングで、EMD サービスセンタ 1 0 2 に送信される。

【 0 2 3 5 】

ステップ S 5 5 - 1 9 : コンテンツ鍵データ $K c$ および利用制御データ 1 6 6

が、作業用メモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED2} および購入者鍵データ K_{PIN} を用いて順に暗号化され、メディアSAM管理部197に出力される。

また、作業用メモリ200からメディアSAM管理部197に、キーファイルKFが出力される。

【0236】

ステップS55-20：メディアSAM管理部197において、図44(C)に示すキーファイル KF_1 が作成され、キーファイル KF_1 がメディアSAM管理部197を介してRAM型の記録媒体130₅のメディアSAM133に書き込まれる。

また、メディアSAM管理部197を介して、キーファイルKFがRAM型の記録媒体130₅のメディアSAM133に書き込まれる。

【0237】

ステップS55-21：SAM105₂のCPU1100は、上述した処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。

なお、CPU1100は、上述した処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0238】

以下、SAM105₁～105₄の実現方法について説明する。

SAM105₁～105₄の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図22に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0239】

例えば、図22に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。

また、図22に示す記憶部192や、図22に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105₁～105₄に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。

また、SAM105₁～105₄には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0240】

上述したように、SAM105₁～105₄は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM105₁～105₄を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU(Memory Management Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。

また、SAM105₁～105₄は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

SAM105₁ ~ 105₄ 自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0241】

SAM105₁ ~ 105₄ の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理を行う場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（MiniOS）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0242】

次に、図22に示すAV圧縮・伸長用SAM163について説明する。

図22に示すように、AV圧縮・伸長用SAM163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。

相互認証部220は、AV圧縮・伸長用SAM163がSAM105₁ からデータを入力する際に、図30に示す相互認証部170との間で相互認証を行ってセッション鍵データK_{SES} を生成する。

【0243】

復号部221は、SAM105₁ から入力したコンテンツ鍵データK_c、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテ

ンツデータCを、セッション鍵データ K_{SES} を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データ K_c およびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0244】

復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データ K_c を用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

また、復号部222は、通常動作時にコンテンツデータCの全体をコンテンツ鍵データ K_c で復号する。

【0245】

伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。

伸長部223は、例えば、図3(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0246】

電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータCを再生するときに、AV圧縮・伸長用SAM163において埋め込まれる。

なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0247】

半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを

復号部 2 2 2 に指示する。

また、半開示処理部 2 2 5 は、その他に、半開示パラメータデータ 1 9 9 に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【0 2 4 8】

再生モジュール 1 6 9 は、復号および伸長されたコンテンツデータ C に応じた再生を行う。

【0 2 4 9】

以下、SAM 1 0 5₁ ～ 1 0 5₄ の出荷時における EMD サービスセンタ 1 0 2 への登録処理について説明する。

なお、SAM 1 0 5₁ ～ 1 0 5₄ の登録処理は同じであるため、以下、SAM 1 0 5₁ の登録処理について述べる。

SAM 1 0 5₁ の出荷時には、EMD サービスセンタ 1 0 2 の鍵サーバ 1 4 1 によって、SAM 管理部 1 4 9 を介して、図 3 0 などに示す記憶部 1 9 2 に以下に示す鍵データが初期登録される。

また、SAM 1 0 5₁ には、例えば、出荷時に、記憶部 1 9 2 などに、SAM 1 0 5₁ が EMD サービスセンタ 1 0 2 に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部 1 9 2 には、例えば、図 3 4 において左側に「*」が付されている SAM 1 0 5₁ の識別子 SAM_ID、記録用鍵データ K_{STR}、ルート認証局 2 の公開鍵データ K_{R-CA}、EMD サービスセンタ 1 0 2 の公開鍵データ K_{ESC,P}、SAM 1 0 5₁ の秘密鍵データ K_{SAM1,S}、公開鍵証明書データ C E R_{SAM1} およびその署名データ S I G_{22,ESC}、A V 圧縮・伸長用 SAM 1 6 3 およびメディア SAM との間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データ C E R_{SAM1} は、SAM 1 0 5₁ を出荷後に登録する際に EMD サービスセンタ 1 0 2 から SAM 1 0 5₁ に送信してもよい。

【0 2 5 0】

また、記憶部 1 9 2 には、SAM 1 0 5₁ の出荷時に、図 3 に示すコンテンツ

ファイルCFおよびキーファイルKFを読み込み形式を示すファイルリーダーが、EMDサービスセンタ102によって書き込まれる。

SAM105₁では、コンテンツファイルCFおよびキーファイルKFに格納されたデータを利用する際に、記憶部192に記憶されたファイルリーダーが用いられる。

【0251】

ここで、ルート認証局2の公開鍵データ K_{R-CA} は、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データ K_{R-CA} は、図1に示すルート認証局2によって発行される。

また、EMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ は、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データ $K_{ESC,P}$ は192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データ $K_{ESC,P}$ を登録する。

また、ルート認証局92は、公開鍵データ $K_{ESC,P}$ の公開鍵証明書データ $CER_{R_{ESC}}$ を作成する。公開鍵データ $K_{ESC,P}$ を格納した公開鍵証明書データ CER_{ESC} は、好ましく、SAM105₁の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データ CER_{ESC} は、ルート認証局92の秘密鍵データ $K_{ROOT,S}$ で署名されている。

【0252】

EMDサービスセンタ102は、乱数を発生してSAM105₁の秘密鍵データ $K_{SAM1,S}$ を生成し、これとペアとなる公開鍵データ $K_{SAM1,P}$ を生成する。

また、EMDサービスセンタ102は、ルート認証局92の認証をもらって、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を発行し、これに自らの秘密鍵データ $K_{ESC,S}$ を用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンドCA（認証局）として機能を果たす。

【0253】

また、SAM105₁には、EMDサービスセンタ102により、EMDサー

ビスセンタ 102 の管理下にある一意（ユニーク）な識別子 SAM_ID が割り当てられ、これが SAM105₁ の記憶部 192 に格納されると共に、EMD サービスセンタ 102 によって管理される。

【0254】

また、SAM105₁ は、出荷後、例えば、ユーザによって EMD サービスセンタ 102 と接続され、登録手続を行うと共に、EMD サービスセンタ 102 から記憶部 192 にライセンス鍵データ KD₁ ~ KD₃ が転送される。

すなわち、SAM105₁ を利用するユーザは、コンテンツをダウンロードする前に EMD サービスセンタ 102 に登録手続が必要である。この登録手続は、例えば、SAM105₁ を搭載している機器（当該例では、ネットワーク機器 160₁）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報（ユーザの氏名、住所、連絡先、性別、決済口座、ログイン名、パスワードなど）を記載して例えば郵便などのオフラインで行なわれる。

SAM105₁ は、上述した登録手続を経た後でないと使用できない。

【0255】

EMD サービスセンタ 102 は、SAM105₁ のユーザによる登録手続に応じて、ユーザに固有の識別子 USER_ID を発行し、例えば、SAM_ID と USER_ID との対応関係を管理し、課金時に利用する。

また、EMD サービスセンタ 102 は、SAM105₁ のユーザに対して情報参照用識別子 ID と、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子 ID とパスワードとを用いて、EMD サービスセンタ 102 に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、EMD サービスセンタ 102 は、ユーザの登録時に、クレジットカード会社などに身分の確認を行ったり、オフラインで本人の確認を行なう。

【0256】

次に、図 34 に示すように、SAM105₁ 内の記憶部 192 に SAM 登録リストを格納する手順について説明する。

図 1 に示す SAM105₁ は、例えば、バス 191 として IEEE 1394 シ

リアルバスを用いた場合に、バス 191 に接続された機器の電源を立ち上げたり、新しい機器をバス 191 に接続したときに生成されるトポロジーマップを利用して、自分の系に存在する SAM105₂ ~ SAM105₄ の SAM 登録リストを得る。

なお、IEEE 1394 シリアルバスであるバス 191 に応じて生成されたトポロジーマップは、例えば、図 58 に示すように、バス 191 に SAM105₁ ~ 105₄ に加えて AV 機器 160₅ , 160₆ の SCMS 処理回路 105₅ , 105₆ が接続されている場合に、SAM105₁ ~ 105₄ および SCMS 処理回路 105₅ , 105₆ を対象として生成される。

従って、SAM105₁ は、当該トポロジーマップから、SAM105₁ ~ 105₄ についての情報を抽出して図 59 に示す SAM 登録リストを生成する。

【0257】

そして、SAM105₁ は、図 59 に示す SAM 登録リストを、EMD サービスセンタ 102 に登録して署名を得る。

これらの処理は、バス 191 のセッションを利用して SAM105₁ が自動的にを行い、EMD サービスセンタ 102 に SAM 登録リストの登録命令を発行する。

EMD サービスセンタ 102 は、SAM105₁ から図 59 に示す SAM 登録リストを受けると、有効期限を確認する。そして、EMD サービスセンタ 102 は、登録時に SAM105₁ より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMD サービスセンタ 102 は、予め保持している図 60 に示すリボケーションリスト CRL をチェックして SAM 登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由に EMD サービスセンタ 102 によって使用が禁止されている（無効な）SAM のリストである。各 SAM は他の SAM と通信を行う際に、リボケーションリストによって通信相手の SAM が無効にされている場合には、当該通信相手の SAM との通信を停止する。

また、EMD サービスセンタ 102 は、決済時には SAM105₁ に対応する SAM 登録リストを取り出し、その中に記述された SAM がリボケーションリス

トに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。

これにより、図61に示すSAM登録リストが作成される。

なお、SAMリボケーションリストは、同一系の（同一のバス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

【0258】

なお、リボケーションリストCRLの更新は、例えば、EMDサービスセンタ102からSAMに放送される更新データに応じて、SAM内部で自動的に行なうことが好ましい。

【0259】

以下、SAMが持つセキュリティ機能について説明する。

SAMは、セキュリティに関する機能として、共通鍵暗号方式のDES（Triple DES/AES）、公開鍵暗号方式の楕円曲線暗号（署名生成／検証ECDSA、共有鍵生成ECDH、公開鍵暗号EC-Elgamal）、圧縮関数のハッシュ関数SHA-1、乱数生成器（真性乱数）の暗号ライブラリーのIP部品を有している。

相互認証、署名生成、署名検証、共有鍵（セッション鍵）作成（配送）には公開鍵暗号方式（楕円曲線暗号）が用いられ、コンテンツの暗号、復号には共通鍵暗号（DES）が用いられ、署名生成、検証の中のメッセージ認証に圧縮関数（ハッシュ関数）が用いられる。

【0260】

図62は、SAMが持つセキュリティ機能を説明するための図である。

SAMが管理するセキュリティー機能は、コンテンツに関連する暗号、復号処理をつかさどるアプリケーション層でのセキュリティー機能（1）と、通信相手と相互認証をしてセキュアな通信路を確保する物理層のセキュリティー機能（2）との2種類がある。

EMDシステム100では、配信されるコンテンツデータCはすべて暗号化され、決済と同時に鍵の購入手続きをすることを前提としている。権利書データ1

0 6 は、コンテンツデータ C と一緒にイン・バンド方式で送られることを前提としているので、ネットワークの媒体と関係のない層でそのデータが管理され、衛星、地上波、ケーブル、無線、記録媒体（メディア）などの流通経路によらず、共通な権利処理システムを提供できる。具体的には、権利書データ 1 0 6 をネットワークの物理層のプロトコルのヘッダに挿入したりすると、使用するネットワークによって、挿入するデータが同じでも、ヘッダのどこに挿入するかを各々のネットワークで決めないといけない。

【 0 2 6 1 】

本実施形態では、コンテンツデータ C およびキーファイル K F の暗号化は、アプリケーション層での保護を意味している。相互認証は、物理層やトランスポート層で行ってもよいし、アプリケーション層で行ってもよい。物理層に暗号機能を組み込むことは、使用するハードウェアに暗号機能を組み込むことを意味している。送信、受信の両者間のセキュアの通信路を確保することが相互認証の本来の目的なので物理層で実現できることが望ましいが、実際はトランスポート層で実現し、伝送路によらないレベルでの相互認証が多い。

【 0 2 6 2 】

S A M が実現するセキュリティ機能には、通信先の相手の正当性を確認するための相互認証と、アプリケーション層での課金処理をとともなうコンテンツデータの暗号化および復号とがある。

機器間で通信を行う際の S A M 相互間での相互認証は、通常、アプリケーション層レベルに実装されるが、トランスポート層や物理層などの他のレイヤに実装されてもよい。

物理層に実装する相互認証は、5 C 1 3 9 4 C P (Content Protection) を利用する。1 3 9 4 C P は 1 3 9 4 L I N K I C (ハードウェア) の Isochronous Channel に共通鍵暗号である M 6 が実装されており、Asynchronous Channel による相互認証（楕円曲線暗号、ハッシュ関数を利用した共通鍵暗号）の結果、生成されるセッション鍵を Isochronous Channel の M 6 に転送し、M 6 による共通鍵暗号を実現する。

【0 2 6 3】

SAM相互間の相互認証を物理層のハードウェア上に実装する場合には、公開鍵暗号（楕円曲線暗号）を利用した相互認証で生成されたセッション鍵をホストCPUを介して1394 LINK ICのM6に転送し、1394 CPで生成されたセッション鍵と併用してコンテンツデータの暗号化を行う。

また、SAM相互間の相互認証をアプリケーション層で行う場合には、SAM内部の共通鍵暗号ライブラリ(DES/Triple DES/AES)を使って暗号化を行う。

【0 2 6 4】

本実施形態では、例えば、SAM相互間の相互認証をアプリケーション層に実装し、1394 CPによる相互認証を1394 LINK ICという物理層（ハードウェア）に実装する。

この場合に、課金処理をともなうコンテンツデータの暗号化および復号はアプリケーション層で行われるが、アプリケーション層は一般ユーザから簡単にアクセスでき、時間無制限に解析される可能性があるため、当該課金処理をともなう処理に関しては、本実施形態では、外部から処理内容をいっさいモニタ（監視）できない耐タンパ性をもったハードウェア内部で行っている。これがSAMを耐タンパ性の構造を持ったハードウェアで実現する最大の理由である。

なお、当該課金処理をホストCPU内で行う場合は、CPUに耐タンパ性のソフトウェアを実装する。

【0 2 6 5】

以下、図1に示すユーザホームネットワーク103内の例えばネットワーク機器160₁ 内の各種のSAMに搭載形態の一例を図63を参照しながら説明する。

図63に示すように、ネットワーク機器160₁ 内には、ホストCPU810₁、SAM105₁、ダウンロードメモリ167、メディア・ドラブSAM260、ドライブCPU1003、DRAMなどのショックプルーフ(Shock Proof: 耐振動用)メモリ1004を有する。

ダウンロードメモリ167と、ショックプルーフメモリ1004の一部の記憶領域は、SAM105₁ およびホストCPU810₁ の双方からアクセス可能な

共有メモリとして用いられる。

ショックブーフメモリ 1004 は、データバス 1002 を介して入力したコンテンツデータを蓄積した後に AV 圧縮・伸長用 SAM163 に出力することで、記録媒体 130 からのコンテンツデータの読み出し動作が振動などに要因で途切れた場合でも、AV 圧縮・伸長用 SAM163 に連続してコンテンツデータ C を出力することを可能にする。これによって、コンテンツデータの再生出力が途切れることが効果的に回避される。

【0266】

ダウンロードメモリ 167 は、メモリコントローラ、バスアービターおよびブリッジの機能を持つモジュール 1005 を介して、ホスト CPU バス 1000 に接続されている。

図 64 は、モジュール 1005 の内部およびその周辺の構成を詳細に示した図である。

図 64 に示すように、モジュール 1005 は、コントローラ 1500 およびバスアービタ／バスブリッジ 1501 を有する。

コントローラ 1500 は、ダウンロードメモリ 167 として DRAM を用いた場合に、DRAM I/F として機能し、ダウンロードメモリ 167 との間に r/w 線、アドレスバス、CAS 線および RAS 線を有している。

バスアービタ／バスブリッジ 1501 は、ホスト CPU バス 1000 のアービトレーション等を行い、ダウンロードメモリ 167 との間にデータバスを有し、コントローラ 1500 との間に r/w 線、アドレスバスおよび Ready 線を有し、SAM1051 との間に CS (Chip Select) 線、r/w 線、アドレスバス、データバスおよび Ready 線を有し、ホスト CPU バス 1000 に接続されている。

ホスト CPU バス 1000 には、バスアービタ／バスブリッジ 1501、ホスト CPU 810₁ および SAM1051 が接続されている。

ホスト CPU バス 1000 は、CS 線、r/w 線、アドレスバス、データバスおよび Ready 線を有する。

【0 2 6 7】

ダウンロードメモリ 1 6 7 およびショックプーフメモリ 1 0 0 4 には、前述したコンテンツファイル C F およびキーファイル K F などが記憶される。

ショックプーフメモリ 1 0 0 4 の記憶領域のうち共有メモリとしては用いられる記憶領域以外の記憶領域は、データバス 1 0 0 2 を介してメディア・ドラブ S A M 2 6 0 から入力したコンテンツデータを A V 圧縮・伸長用 S A M 1 6 3 に出力するまで一時的に記憶するために用いられる。

【0 2 6 8】

A V 圧縮・伸長用 S A M 1 6 3 は、ホスト C P U バス 1 0 0 0 を介してダウンロードメモリ 1 6 7 との間でデータ転送を行い、データバス 1 0 0 2 を介してメディア・ドラブ S A M 2 6 0 との間でデータ転送を行う。

【0 2 6 9】

ホスト C P U バス 1 0 0 0 には、ダウンロードメモリ 1 6 7 の他に、S A M 1 0 5₁、A V 圧縮・伸長用 S A M 1 6 3 および D M A (Direct Memory Access) 1 0 1 0 が接続されている。

D M A 1 0 1 0 は、ホスト C P U バス 1 0 0 0 を介したダウンロードメモリ 1 6 7 へのアクセスを、ホスト C P U 8 1 0₁ からの命令に応じて、統括的に制御する。

また、ホスト C P U バス 1 0 0 0 は、1 3 9 4 シリアル・インターフェースの L I N K 層を用いてユーザホームネットワーク 1 0 3 内の他の S A M 1 0 5₂ ~ 1 0 5₄ と通信を行なう際に用いられる。

【0 2 7 0】

ドライブ C P U バス 1 0 0 1 には、ドライブ C P U 1 0 0 3、メディア・ドラブ S A M 2 6 0、R F アンプ 1 0 0 6、メディア S A M インターフェイス 1 0 0 7 および D M A 1 0 1 1 が接続されている。

ドライブ C P U 1 0 0 3 は、例えば、ホスト C P U 8 1 0₁ からの命令を受けて、ディスク型の記録媒体 1 3 0 にアクセスを行う際の処理を統括的に制御する。この場合に、ホスト C P U 8 1 0₁ がマスタとなり、ドライブ C P U 1 0 0 3 がスレーブとなる。ドライブ C P U 1 0 0 3 は、ホスト C P U 8 1 0₁ から見て

I/Oとして扱われる。

ドライブCPU1003は、例えばRAM型などの記録媒体130にアクセスを行う際のデータのエンコードおよびデコードを行う。

ドライブCPU1003は、RAM型の記録媒体130がドライブにセットされると、RAM型の記録媒体130がSAM105₁による権利処理の対象となる（EMDシステム100の対象となる）記録媒体であるか否かを判断し、当該記録媒体であると判断した場合に、そのことをホストCPU810₁に通知すると共に、メディア・ドラブSAM260にメディアSAM133との間の相互認証などを行うことを指示する。

【0271】

メディアSAMインターフェイス1007は、ドライブCPUバス1001を介した記録媒体130のメディアSAM133に対してのアクセスを行う際のインターフェイスとして機能する。

DMA1011は、例えば、ドライブCPU1003からの命令に応じて、ドライブCPUバス1001およびデータバス1002を介したショックプルフメモリ1004へのメモリアccessを統括的に制御する。DMA1011は、例えば、データバス1002を介した、メディア・ドラブSAM260とショックプルフメモリ1004との間のデータ転送を制御する。

【0272】

図63に示す構成では、例えば、SAM105₁と記録媒体130のメディアSAM133との間で相互認証などの通信を場合には、ホストCPU810₁の制御に基づいて、ホストCPUバス1000、ホストCPU810₁、ドライブCPU1003内のレジスタ、ドライブCPUバス1001およびメディアSAMインターフェイス1007を介して、SAM105₁とメディアSAM133との間でデータが転送される。

また、記録媒体130にアクセスを行う場合には、メディア・ドラブSAM260とメディアSAM133との間で相互認証が行われる。

また、前述したように、ダウンロードメモリ167およびショックプルフメモリ1004にアクセスを行うために、AV圧縮・伸長用SAM163において

データを圧縮または伸長する場合には、SAM105₁ とAV圧縮・伸長用SAM163との間で相互認証が行われる。

【0273】

本実施形態では、図63において、SAM105₁ およびAV圧縮・伸長用SAM163は、ホストCPU810₁ からは、I/Oインターフェイスに接続されたデバイスとして扱われる。SAM105₁ およびAV圧縮・伸長用SAM163とホストCPU810₁ との間の通信およびデータ転送は、メモリI/O&アドレスデコーダ1020の制御に基づいて行われる。このとき、ホストCPU810₁ がマスタ(Master)になり、SAM105₁ およびAV圧縮・伸長用SAM163がスレーブ(Slave)になる。SAM105₁ およびAV圧縮・伸長用SAM163は、ホストCPU810₁ からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をホストCPU810₁ に通知する。

また、メディアSAM133およびメディア・ドラブSAM260は、ドライブCPU1003からはI/Oインターフェイスに接続されたデバイスとして扱われる。メディアSAM133およびメディア・ドラブSAM260とドライブCPU1003との間の通信およびデータ転送は、メモリI/O&アドレスデコーダ1021の制御に基づいて行われる。このとき、ドライブCPU1003がマスタになり、メディアSAM133およびメディア・ドラブSAM260がスレーブになる。メディアSAM133およびメディア・ドラブSAM260は、ドライブCPU1003からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をドライブCPU1003に通知する。

【0274】

また、ダウンロードメモリ167およびショックブーフメモリ1004に対してのコンテンツファイルCFおよびキーファイルKFに関するアクセス制御は、SAM105₁ が統括的に行ってもよいし、あるいはコンテンツファイルCFのアクセス制御をホストCPU810₁ が行い、キーファイルKFのアクセス制御をSAM105₁ が行ってもよい。

【0275】

ドライブCPU1003によって記録媒体130から読み出されたコンテンツ

データCは、RFアンプ1006およびメディア・ドラブSAM260を経て、ショックプーフメモリ1004に格納され、その後、AV圧縮・伸長用SAM163において伸長される。伸長されたコンテンツデータはD/A変換器において、2でデジタルからアナログに変換され、当該変換によって得られたアナログ信号に応じた音響がスピーカから出力される。

このとき、ショックプーフメモリ1004は、記録媒体130の離散的に位置する記録領域から非連続的に読み出された複数のトラックのコンテンツデータCを一時的に格納した後に、AV圧縮・伸長用SAM163に連続して出力してもよい。

【0276】

以下、図63に示すユーザホームネットワーク103内の各種のSAMのマスター・スレーブ関係を説明する。

例えば、購入形態を決定したコンテンツデータを記録媒体130に記録する場合には、図65に示すように、ホストCPU810₁が、そのI/OデバイスであるSAM105₁に、当該コンテンツデータの購入形態決定を行う旨を内部割り込みによって指示すると共に、記録媒体130のメディアSAM133と相互認証を行って、記録媒体130にコンテンツデータを記録する。

このとき、ホストCPU810₁がマスターとなり、SAM105₁および記録媒体130がスレーブとなる。記録媒体130も、ホストCPU810₁からはI/Oデバイスとして扱われる。

SAM105₁は、ホストCPU810₁から上記内部割り込みを受けると、記録媒体130のメディアSAM133と通信を行って、コンテンツデータの購入形態を決定すると共に、コンテンツ鍵データKcなどの所定の鍵データをメディアSAM133に書き込む。そして、SAM105₁は、当該処理が終了すると、ホストCPU810₁に対しての外部割り込み、あるいはホストCPU810₁からのポーリングによって、当該処理の結果をホストCPU810₁に通知する。

【0277】

また、例えば、記録媒体に記録された既に購入形態が決定されたコンテンツデ

ータの再生を行う場合には、図 6 6 に示すように、ホスト CPU 8 1 0₁ から SAM 1 0 5₁ に対して、当該再生を行う旨の指示が内部割り込みによって出される。

SAM 1 0 5₁ は、当該内部割り込みを受けると、記録媒体 1 3 0 のメディア SAM 1 3 3 からキーファイル KF などの鍵データブロックを読み出し、当該鍵データブロックに格納された利用制御データ 1 6 6 などに基づいて、コンテンツデータの再生処理を行う。

SAM 1 0 5₁ は、AV 圧縮・伸長用 SAM 1 6 3 に、記録媒体 1 3 0 から読み出したコンテンツデータの伸長処理を行う旨の指示を内部割り込みによって出す。

AV 圧縮・伸長用 SAM 1 6 3 は、当該内部割り込みを SAM 1 0 5₁ から受けると、記録媒体 1 3 0 から読み出したコンテンツデータのデスクランブル処理、電子透かし情報の埋め込み処理および検出処理、並びに伸長処理を行った後に、当該コンテンツデータを D/A 変換回路などを介して出力して再生を行う。

そして、AV 圧縮・伸長用 SAM 1 6 3 は、当該再生処理が終了すると、その旨を SAM 1 0 5₁ に通知する。

SAM 1 0 5₁ は、AV 圧縮・伸長用 SAM 1 6 3 から、当該再生処理が終了した旨の通知を受けると、その旨を外部割り込み等でホスト CPU 8 1 0₁ に通知する。

この場合に、ホスト CPU 8 1 0₁ と SAM 1 0 5₁ との関係では、ホスト CPU 8 1 0₁ がマスタとなり、SAM 1 0 5₁ がスレーブとなる。

また、SAM 1 0 5₁ と AV 圧縮・伸長用 SAM 1 6 3 との関係では、SAM 1 0 5₁ がマスタとなり、AV 圧縮・伸長用 SAM 1 6 3 がスレーブとなる。

また、上述した実施形態では、AV 圧縮・伸長用 SAM 1 6 3 を SAM 1 0 5₁ のスレーブとなるようにしたが、AV 圧縮・伸長用 SAM 1 6 3 をホスト CPU 8 1 0₁ のスレーブとなるようにしてもよい。

【0 2 7 8】

また、例えば、コンテンツデータの権利処理を行うことなく、記録媒体 1 3 0 に記録されたコンテンツデータの再生処理を行う場合には、図 6 7 に示すように

、ホストCPU 810₁ からAV圧縮・伸長用SAM 163に、内部割り込みによって、再生処理を行う旨の指示が出される。また、ホストCPU 810₁ からメディア・ドラブSAM 260に、内部割り込みによって、記録媒体130からコンテンツデータを読み出す旨の指示が出される。

メディア・ドラブSAM 260は、上記内部割り込みを受けると、記録媒体130から読み出したコンテンツデータをデコード部でデコードした後に、ショックブーフメモリ1004に格納する。そして、メディア・ドラブSAM 260は、当該処理を終了すると、その旨を外部割り込みによってホストCPU 810₁ に通知する。

ショックブーフメモリ1004に格納されたコンテンツデータは、AV圧縮・伸長用SAM 163によって読み出され、AV圧縮・伸長用SAM 163において、デスクランブル処理、電子透かし情報の埋め込み処理および検出処理、並びに伸長処理を行った後に、D/A変換回路などを介して再生出力される。

AV圧縮・伸長用SAM 163は、当該再生処理が終了すると、その旨を外部割り込みによってホストCPU 810₁ に通知する。

この場合に、ホストCPU 810₁ がマスタとなり、AV圧縮・伸長用SAM 163およびメディア・ドラブSAM 260がスレーブとなる。

【0279】

以下、ユーザホームネットワーク103内の各種のSAMが上述した機能を実現するために備える回路モジュールについて説明する。

ユーザホームネットワーク103内のSAMとしては、前述したように、購入形態の決定などの権利処理（利益分配）に係わる処理を行うSAM 105（105₁～105₄）と、記録媒体に設けられるメディアSAM 133と、AV圧縮・伸長用SAM 163と、メディア・ドラブSAM 260とがある。以下、これらのSAMに設けられる回路モジュールをそれぞれ説明する。

【0280】

<権利処理用のSAMの第1形態>

図68は、権利処理用のSAM 105aの回路モジュールを説明するための図である。

図 68 に示すように、SAM105a は、CPU1100、DMA1101、MMU1102、I/O モジュール 1103、マスク ROM1104、不揮発性メモリ 1105、作業用 RAM1106、公開鍵暗号モジュール 1107、共通鍵暗号モジュール 1108、ハッシュ関数モジュール 1109、(真性) 乱数発生器 1110、リアルタイムクロックモジュール 1111、外部バス I/F 1112 を有する耐タンパ性のハードウェア (Tamper Resistant H/W) (本発明の回路モジュール) である。

ここで、CPU1100 が本発明の演算処理回路に対応し、マスク ROM1104、不揮発性メモリ 1105 および作業用 RAM1106 が本発明の記憶回路に対応し、共通鍵暗号モジュール 1108 が本発明の暗号処理回路に対応し、外部バス I/F 1112 が本発明の外部バスインターフェイスに対応している。

また、後述する図 64 の内部バス 1120、1121 が本発明の第 1 のバスに対応し、外部バス 1123 が本発明の第 2 のバスに対応している。

また、内部バス 1120 が本発明の第 3 のバスに対応し、内部バス 1121 が本発明の第 4 のバスに対応している。

また、外部バス I/F 1112 が本発明の第 1 のインターフェイス回路に対応し、バス I/F 回路 1116 が本発明の第 2 のインターフェイス回路に対応している。

また、内部バス 1122 が本発明の第 5 のバスに対応し、I/O モジュールが本発明の第 3 のインターフェイス回路に対応し、バス I/F 回路 1117 が本発明の第 4 のインターフェイス回路に対応している。

【0281】

図 30 に示す SAM105₁ の機能モジュールと、図 68 に示す回路モジュールとの関係を簡単に説明する。

CPU1100 は、例えば、マスク ROM1104 および不揮発性メモリ 1105 に記憶されたプログラムを実行して、図 30 に示す CPU1100、課金処理部 187 および利用監視部 186 の機能を実現する。

DMA1101 は、CPU1100 からの命令に応じて、図 22 に示すダウンロードメモリ 167 および図 30 に示す記憶部 192 に対してのアクセスを統括

的に制御する。

MMU 1102は、図22に示すダウンロードメモリ167および図30に示す記憶部192のアドレス空間を管理する。

I/Oモジュール1103は、例えば、図30に示すメディアSAM管理部197の一部の機能を実現する。

マスクROM1104には、SAM105aの初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムおよびデータが製造時に記憶され、図30に示す記憶部192の一部の機能を実現する。

不揮発性メモリ1105は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶し、図30に示す記憶部192の一部の機能を実現する。

作業用RAM1106は、図30に示す作業用メモリ200に対応している。

【0282】

公開鍵暗号モジュール1107は、図30に示す署名処理部189の機能の一部を実現し、例えば、公開鍵暗号方式を用いた、メディアSAM133等と間の相互認証、SAM105の署名データの作成、署名データ(EMDサービスセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサービスプロバイダ310の署名データ)の検証、データ量の少ないデータ(キーファイルKFなど)の転送を行う際の当該データの暗号化および復号、並びに、鍵共有を行う際に用いられる。公開鍵暗号モジュール1107は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1105に記憶した公開鍵暗号プログラムをCPU1100において実行して実現してもよい(S/W IP Solution)。

【0283】

共通鍵暗号モジュール1108は、図30に示す署名処理部189、暗号化・復号部171, 172, 173の機能の一部を実現し、相互認証、相互認証によって得た共通鍵であるセッション鍵データ K_{SES} を用いたデータの暗号化および復号を行う際に用いられる。共通鍵暗号方式は、公開鍵暗号方式に比べて高速処理が可能であり、例えば、コンテンツデータ(コンテンツファイルCF)などの

データ量が大きいデータを暗号化および復号する際に用いられる。共通鍵暗号モジュール 1108 は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ 1105 に記憶した共通鍵暗号プログラムを CPU 1100 において実行して実現してもよい(S/W IP Solution)。

なお、相互認証は、公開鍵暗号モジュール 1107 による暗号・復号および共通鍵暗号モジュール 1108 による暗号・復号の何れか一方あるいは双方を採用する。

また、共通鍵暗号モジュール 1108 は、コンテンツ鍵データ K_c をライセンス鍵データ K_D を用いて復号する。

【0284】

ハッシュ関数モジュール 1109 は、図 30 に示す署名処理部 189 の機能の一部を実現し、署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール 1109 は、コンテンツプロバイダ 101 および EMD サービスセンタ 102 などの署名データや、図 44 に示すセキュアコンテナ 104x のキーファイル K_{F1} のハッシュ値 H_{K1} を検証する際に用いられる。ハッシュ関数モジュール 1109 は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ 1105 に記憶したハッシュ回路モジュールを CPU 1100 において実行して実現してもよい(S/W IP Solution)。

【0285】

乱数発生器 1110 は、例えば、図 30 に示す相互認証部 170 の機能の一部を実現する。

リアルタイムクロックモジュール 1111 は、リアルタイムの時刻を発生する。当該時刻は、例えば、有効期限付きのライセンス鍵データ K_D を選択する場合や、利用制御データ 166 によって示される有効期限の要件を満たされているかを判断する際に用いられる。

外部バス I/F 1112 は、図 30 に示すコンテンツプロバイダ管理部 180、ダウンロードメモリ管理部 182 および EMD サービスセンタ管理部 185 の一部を機能を実現する。

【0286】

図69は、SAM105a内のハードウェア構成を説明するための図である。

図69において、図68に示したものと同一回路モジュールには、図68と同じ符号を付している。

図69に示すように、SAM105a内では、SAM・CPUバス1120を介してCPU1100、マスクROM1104および不揮発性メモリ1105が接続されている。

内部バス1121には、DMA1101が接続されている。

内部バス1122には、I²C・インターフェイス1130、メディアSAM・インターフェイス1131、MS(Memory Stick)・インターフェイス1132およびICカード・インターフェイス1133が接続されている。

メディアSAM・インターフェイス1131は記録媒体130のメディアSAM133との間でデータ転送を行う。MS・インターフェイス1132はメモリスティック1140との間でデータ転送を行う。ICカード・インターフェイス1133はICカード1141との間でデータ転送を行う。

【0287】

外部バス1123には、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、乱数発生器1110、リアルタイムクロック生成モジュール1111、外部バスI/F.1112および外部メモリI/F1140が接続されている。

外部バスI/F1112は、図63に示す外部メモリ201が接続される。

外部メモリI/F1140は、図63に示すホストCPUバス1000に接続される。

【0288】

SAM・CPUバス1120と内部バス1121とは、バス・インターフェイス1116を介して接続されている。

内部バス1122と内部バス1121とは、バス・インターフェイス1117を介して接続されている。

内部バス1121と外部バス1123とは、バス・インターフェイス1115

を介して接続されている。

【0289】

バス・インターフェイス 1115 内には、SRAM 1155 および SAM ステータスレジスタ 1156 が設けられている。

SRAM 1155 は、後述するように、

SAM ステータスレジスタ 1156 には、前述したように、第 1 の SAM ステータスレジスタおよび第 2 の SAM ステータスレジスタがある。第 1 の SAM ステータスレジスタには、ホスト CPU 810₁ によって読み出される、SAM 105₁ のステータス（状態）を示すフラグが設定される。第 2 の SAM ステータスレジスタには、ホスト CPU 810₁ からタスク実行の依頼が出されているか否かのステータスを SAM 105₁ の内部の CPU から読みに行くフラグが設定される。

【0290】

DMA 1101 は、CPU 1100 からの命令に応じて、内部バス 1121 を介した、マスク ROM 1104、不揮発性メモリ 1105 および作業用 RAM 1106 に対してのアクセスを統括的に制御する。

MMU 1113 は、マスク ROM 1104、不揮発性メモリ 1105、作業用 RAM 1106、図 63 に示すダウンロードメモリ 167 のメモリ空間を管理する。

アドレスデコーダ 1114 は、内部バス 1121 と外部バス 1123 との間でデータ転送を行う際に、アドレス変換を行う。

また、書き込みロック制御回路 1135 は、CPU 1100 からのロック鍵データに基づいて、フラッシュ ROM に対してのデータの書き込みおよび消去をブロック単位で管理する。

【0291】

次に、権利処理用の SAM 105 a のアドレス空間を説明する。

図 70 は、権利処理用の SAM 105 a のアドレス空間を説明するための図である。

図 70 に示すように、権利処理用の SAM 105 a のアドレス空間には、開始

アドレスから順に、例えば、ブートプログラム、システムコンフィギュレーション、フラッシュROM、所定のプログラム、フラッシュROMのデバイスドライバ、不揮発性メモリのデバイスドライバ、図69に示す作業用RAM1106、所定のプログラム、作業用RAM1106、所定のプログラム、図69に示すSRAM1155、外部メモリ201、Key__TOC/File__System、SAM登録リスト、利用履歴データ108、図69に示す共通鍵暗号モジュール1108のレジスタ、図69に示す公開鍵暗号モジュール1107のレジスタ、図69に示すハッシュ関数モジュール1109のレジスタ、図69に示す乱数発生器1110のレジスタ、図69に示すリアルタイムクロックモジュール1111のレジスタ、現在時刻レジスタ、有効期限レジスタ、コントロールレジスタ、ICカードのインターフェイス、メディアSAMのインターフェイス、メモリスティックのインターフェイス、I²Cバスのインターフェイスに割り当てられている。

【0292】

システムコンフィギュレーションに割り当てられたアドレス空間内には、図69に示すDMA1101およびSAMステータスレジスタ1156が割り当てられている。

また、フラッシュROMに割り当てられたアドレス空間内には、メインルーチン（カーネル）、割り込みプログラム、当該割り込みプログラムによって呼び出されるサブルーチン、コマンド解析部（コマンドと割り込みプログラムの開始アドレスの対応表）、割り込みベクタテーブルが割り当てられている。

図70に示すSAM105aのアドレス空間のうち、SAMステータスレジスタ1156およびSRAM1155は、ホストCPU810との共有メモリ空間として用いられる。

【0293】

次に、図63に示すホストCPU810₁のアドレス空間を説明する。

図71は、図63に示すホストCPU810₁のアドレス空間を説明するための図である。

図71に示すように、ホストCPU810₁のアドレス空間は、開始アドレス

から順に、例えば、ブートプログラム、システムコンフィギュレーション、コードが記憶されるROM、データが記憶されるRAM、作業用RAM、図63に示すSAM105₁との共有メモリ、図63に示すAV圧縮・伸長用SAM163との共有メモリ、図63に示すメディア・ドラブSAM260との共有メモリおよび外部デバイスが割り当てられている。

図63に示すSAM105₁との共有メモリには、図69に示すSRAM1155およびSAMステータスレジスタ1156が割り当てられている。

【0294】

＜権利処理用のSAMの第2形態＞

図72は、権利処理用のSAM105bの回路モジュールを説明するための図である。

図72では、SAM105aの構成要素と同じものには、図69と同じ符号を付している。

図72に示すように、SAM105bは、セキュアメモリ105ba、ホストCPU810、耐タンパ性ソフトウェア1130、I/Oモジュール1103を用いて実現される。

SAM105bでは、ホストCPU810において、耐タンパ性ソフトウェア1130を実行することで、図68に示すCPU1100と同じ機能を実現する。耐タンパ性ソフトウェア1130は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。

セキュアメモリ105baには、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、（真性）乱数発生器1110、リアルタイムクロックモジュール1111および外部バスI/F1112を有する耐タンパ性のハードウェアである。

なお、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108およびハッシュ関数モジュール1109は、回路モジュールとして実現してもよいし(H/W IP Solution)、それぞれ不揮発性メモリ1105に記憶した公開鍵暗号プロ

グラム、共通鍵暗号プログラムおよびハッシュ関数プログラムをホストCPU 810において実行して実現してもよい(S/W IP Solution)。

【0295】

以下、前述したメディアSAM133の構成の一例を説明する。

図73は、メディアSAM133の回路モジュールを説明するための図である。

図73に示すように、メディアSAM133は、CPU1200、DMA1201、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207、共通鍵暗号モジュール1208、ハッシュ関数モジュール1209、(真性)乱数発生器1210を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【0296】

CPU1200は、耐タンパ性のハードウェア内の各回路の制御を行う。

【0297】

作業用RAM1106は、図30に示す作業用メモリ200に対応している。

公開鍵暗号モジュール1207は、例えば、公開鍵暗号方式を用いた、例えば(1):図63に示すSAM105₁およびドライブCPU1003等と間の相互認証、(2)メディアSAM133の署名データの作成、署名データ(EMDサービスセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサービスプロバイダ310の署名データ)の検証、(3):転送されるデータ量の少ないメッセージの暗号化および復号、並びに、(4):相互認証によって得たセッション鍵データ K_{SES} の鍵共有を行う際に用いられる。公開鍵暗号モジュール1107は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1205に記憶した公開鍵暗号プログラムをCPU1200において実行して実現してもよい(S/W IPSolution)。

【0298】

共通鍵暗号モジュール1208は、相互認証、相互認証によって得た共通鍵であるセッション鍵データ K_{SES} を用いたキーファイルKF、 KF_1 などのデータの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール1208は、

回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ 1 2 0 5 に記憶した共通鍵暗号プログラムを CPU 1 2 0 0 において実行して実現してもよい(S/W IP Solution)。

なお、相互認証は、公開鍵暗号モジュール 1 2 0 7 による暗号・復号および共通鍵暗号モジュール 1 2 0 8 による暗号・復号の何れか一方あるいは双方を採用する。

【0 2 9 9】

ハッシュ関数モジュール 1 2 0 9 は、データのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール 1 1 0 9 は、図 4 4 に示すセキュアコンテナ 1 0 4 x のキーファイル KF_1 のハッシュ値 H_{K1} を検証する際に用いられる。ハッシュ関数モジュール 1 2 0 9 は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ 1 2 0 5 に記憶したハッシュ回路モジュールを CPU 1 2 0 0 において実行して実現してもよい(S/W IP Solution)。

【0 3 0 0】

乱数発生器 1 2 1 0 は、例えば、相互認証を行う際に用いられる。

I/Oモジュール 1 2 0 3 は、図 6 3 に示すメディア SAM I/F 1 0 0 7 との間の通信を行う際に用いられる。

【0 3 0 1】

マスク ROM 1 2 0 4 には、メディア SAM 1 3 3 の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムおよびデータが製造時に記憶される。

不揮発性メモリ 1 2 0 5 は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

【0 3 0 2】

図 7 4 は、メディア SAM 1 3 3 が ROM 型の記録媒体に搭載される場合に、メディア SAM 1 3 3 の出荷時にマスク ROM 1 2 0 4 および不揮発性メモリ 1 2 0 5 に格納されているデータを示す図である。

図 7 4 に示すように、ROM 型の記録媒体の出荷時には、メディア SAM 1 3

3には、メディアSAMの識別子（ID）、記録用鍵データ K_{STR} （メディア鍵データ K_{MED} ）、EMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ 、ルート認証局92の公開鍵データ $K_{R-CA,P}$ 、メディアSAM133の公開鍵証明書データ CER_{MSAM} 、メディアSAM133の公開鍵データ $K_{MSAM,P}$ 、メディアSAM133の秘密鍵データ $K_{MSAM,S}$ 、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子（ID）、メディアのタイプ（メディアの種類情報、ROMおよびRAMの何れかを特定する情報）、キーファイルKFの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータC（コンテンツファイルCF）のキーファイルKF、所定の検証値（MAC値）などが記憶される。

ここで、キーファイルKFの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータC（コンテンツファイルCF）のキーファイルKF、並びに所定の検証値（MAC値）は、EMDサービスセンタ102が管理するライセンス鍵データKDを用いて暗号化されている。

【0303】

図75は、メディアSAM133がROM型の記録媒体に搭載される場合に、メディアSAM133の出荷後のユーザ登録およびコンテンツデータの購入形態決定を行ったときにマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。

図75に示すように、メディアSAM133には、ユーザ登録によって、新たに、ユーザID、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報、キーファイル KF_1 などのデータが書き込まれる。

【0304】

図76は、メディアSAM133がRAM型の記録媒体に搭載される場合に、メディアSAM133の出荷時にマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。

図76に示すように、RAM型の記録媒体の出荷時には、メディアSAM133には、メディアSAMの識別子（ID）、記録用鍵データ K_{STR} （メディア鍵

データ K_{MED})、EMDサービスセンタ 102 の公開鍵データ $K_{ESC,P}$ 、ルート認証局 92 の公開鍵データ $K_{R-CA,P}$ 、メディア SAM133 の公開鍵証明書データ CER_{MSAM} 、メディア SAM133 の公開鍵データ $K_{MSAM,P}$ 、メディア SAM133 の秘密鍵データ $K_{MSAM,S}$ 、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子 (ID)、メディアのタイプ (メディアの種類情報、ROM および RAM の何れかを特定する情報) が記憶されており、キーファイル KF の物理アドレス情報 (レジスタ空間のアドレス)、各コンテンツデータ C (コンテンツファイル CF) のキーファイル KF, KF_1 、所定の検証値 (MAC 値) などは記憶されていない。

【0305】

図 77 は、メディア SAM133 が RAM 型の記録媒体に搭載される場合に、メディア SAM133 の出荷後のユーザ登録およびコンテンツデータの購入形態決定処理を行ったときにマスク ROM 1204 および不揮発性メモリ 1205 に格納されているデータを示す図である。

図 73 に示すように、メディア SAM133 には、ユーザ登録によって、新たに、ユーザ ID、パスワード、個人嗜好情報、個人決済情報 (クレジットカード番号など) および電子マネー情報などのデータに加えて、キーファイル KF の物理アドレス情報 (レジスタ空間のアドレス)、各コンテンツデータ C (コンテンツファイル CF) のキーファイル KF, KF_1 、並びに所定の検証値 (MAC 値) が書き込まれる。

キーファイル KF の物理アドレス情報 (レジスタ空間のアドレス)、各コンテンツデータ C (コンテンツファイル CF) のキーファイル KF, KF_1 、並びに所定の検証値 (MAC 値) は、記録用鍵データ K_{STR} によって暗号化されている。

【0306】

＜AV 圧縮・伸長用 SAM163＞

AV 圧縮・伸長用 SAM163 は、例えば、図 22 を用いて説明した機能を実現する。

図 78 は、AV 圧縮・伸長用 SAM163 の回路モジュールを説明するための

図である。

図 78 に示すように、AV 圧縮・伸長用 SAM163 は、CPU/DSP1300、DMA1301、マスク ROM1304、不揮発性メモリ1305、作業用 RAM1306、共通鍵暗号モジュール1308、(真性)乱数発生器1310、圧縮・伸長モジュール1320、電子透かし情報付加・検出モジュール1321 および情報半開示制御モジュール1322 を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【0307】

CPU/DSP1300 は、例えば、図 63 に示す SAM105₁ からの命令に応じて、マスク ROM1304 および不揮発性メモリ1305 に記憶されたプログラムを実行し、AV 圧縮・伸長用 SAM163 内の各回路モジュールを統括的に制御する。

DMA1301 は、CPU/DSP1300 からの命令に応じて、マスク ROM1304、不揮発性メモリ1305、作業用 RAM1306 に対してのアクセスを統括的に制御する。

マスク ROM1304 には、AV 圧縮・伸長用 SAM163 の初期化プログラムやインテグリティチェック(Integrity Check) プログラムなどの改変しないプログラムや、AV 圧縮・伸長用 SAM163 の識別子である AVSAM_ID などの改変しないデータが製造時に記憶される。

不揮発性メモリ1305 は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

作業用 RAM1306 は、SAM105₁ から入力したキーファイル KF などを記憶する。

【0308】

共通鍵暗号モジュール1308 は、SAM105₁ との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データ K_{SES} を用いたコンテンツデータおよびコンテンツ鍵データ K_c などの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール1308 は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1305 に記憶した共通鍵暗号プログラムを

CPU/DSP1300において実行して実現してもよい(S/W IP Solution)。

また、共通鍵暗号モジュール1308は、SAM105₁ から得たコンテンツ鍵データKcを用いて、コンテンツデータCの復号を行う。

乱数発生器1110は、例えば、SAM105₁ との間の相互認証処理を行う際に用いられる。

【0309】

圧縮・伸長モジュール1320は、例えば、図22に示す伸長部223の機能を実現し、図63に示すダウンロードメモリ167およびショックプーフメモリ1004から入力したコンテンツデータの伸長処理と、A/D変換器から入力したコンテンツデータの圧縮処理とを行う。

【0310】

電子透かし情報添付・検出モジュール1321は、図22に示す電子透かし情報処理部224の機能を実現し、例えば、圧縮・伸長モジュール1320の処理対象となるコンテンツデータに対して所定の電子透かし情報を埋め込むと共に、当該コンテンツデータに埋め込まれた電子透かし情報を検出し、圧縮・伸長モジュール1320による処理の適否を判断する。

【0311】

情報半開示制御モジュール1322は、図22に示す半開示処理部225の機能を実現し、必要に応じて、コンテンツデータを半開示状態で再生する。

【0312】

<メディア・ドラブSAM260>

図79は、メディア・ドラブSAM260の回路モジュールを説明するための図である。

図79に示すように、メディア・ドラブSAM260は、CPU1400、DMA1401、マスクROM1404、不揮発性メモリ1405、作業用RAM1406、共通鍵暗号モジュール1408、ハッシュ関数モジュール1409、(真性)乱数発生器1410、エンコーダ・デコーダモジュール1420、記録用鍵データ生成モジュール1430およびメディア・ユニークID生成モジュール1440を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【0313】

CPU1400は、例えば、図63に示すドライブCPU1003からの命令に応じて、マスクROM1404および不揮発性メモリ1405に記憶されたプログラムを実行し、メディア・ドラブSAM260内の各回路モジュールを統括的に制御する。

DMA1401は、CPU1400からの命令に応じて、マスクROM1404、不揮発性メモリ1405、作業用RAM1406に対してのアクセスを統括的に制御する。

マスクROM1404には、メディア・ドラブSAM260の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムや、メディア・ドラブSAM260の識別子であるMDSAM_IDなどの改変しないデータが製造時に記憶される。

不揮発性メモリ1405は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

作業用RAM1406は、種々の処理を行う際の作業用メモリとして用いられる。

【0314】

共通鍵暗号モジュール1408は、メディアSAM133およびAV圧縮・伸長用SAM163との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データ K_{SES} を用いたコンテンツファイルCFおよびキーファイルKFなどの暗号化および復号、並びに記録用鍵データ K_{STR} およびメディア鍵データ K_{MED} を用いたコンテンツ鍵データ K_c の暗号化などを行う際に用いられる。また、共通鍵暗号モジュール1408は、共通鍵データと署名の対象となるデータのハッシュ値を用いて、署名データの検証および作成を行う。

共通鍵暗号モジュール1408は、回路モジュールとして実現してもよい(H/W IPSolution)、不揮発性メモリ1405に記憶した共通鍵暗号プログラムをCPU1400において実行して実現してもよい(S/W IP Solution)。

なお、記録用鍵データ K_{STR} を用いたコンテンツ鍵データ K_c の暗号化は、メディア・ドラブSAM260の共通鍵暗号モジュール1408およびメディアS

AM133の何れで行ってもよい。

ハッシュ関数モジュール1409は、署名データの検証、並びに署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。

乱数発生器1410は、例えば、メディアSAM133との間の相互認証処理を行う際に用いられる。

【0315】

エンコーダ・デコーダモジュール1420は、記録媒体130のROM領域あるいはRAM領域に対して、コンテンツデータのアクセスを行う際に、当該コンテンツデータのエンコード処理、デコード処理、ECC(Error Correction Code)処理、変調処理、復調処理、セクタライズ処理およびデセクタライズ処理などを行う。

【0316】

記録用鍵データ生成モジュール1430は、メディア・ユニークID生成モジュール1440が生成したメディア・ユニークIDを用いて、各メディアにユニークな記録用鍵データ K_{STR} を生成する。

【0317】

メディア・ユニークID生成モジュール1440は、メディア・ドライブSAM260で生成したドライブIDと、メディアSAM133のメディアSAM_IDとから、各記録媒体(メディア)にユニークなメディア・ユニークIDを生成する。

【0318】

以下、図1に示すEMDシステム100の全体動作について説明する。

図80は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1: EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データ K_{CP} の公開鍵証明書 CER_{CP} をコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、 $SAM105_1 \sim 105_4$ が所定の登録処理を経た後に、 $SAM105_1 \sim 105_4$ の公開鍵データ $K_{SAM1,P} \sim K_{SAM4,P}$ の公開鍵証明書 $CER_{CP1} \sim CER_{CP4}$ を $SAM105_1 \sim 105_4$ に送信す

る。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の3カ月分のライセンス鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク103の $SAM105_1 \sim 105_4$ に送信する。

このように、EMDシステム100では、ライセンス鍵データ $KD_1 \sim KD_3$ を予め $SAM105_1 \sim 105_4$ に配給しているため、 $SAM105_1 \sim 105_4$ とEMDサービスセンタ102との間がオフラインの状態でも、 $SAM105_1 \sim 105_4$ においてコンテンツプロバイダ101から配給されたセキュアコンテナ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、 $SAM105_1 \sim 105_4$ とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ166は、原則として、リアルタイムで、 $SAM105_1 \sim 105_4$ からEMDサービスセンタ102に送信される。

【0319】

ステップS2：コンテンツプロバイダ101は、EMDサービスセンタ102との間で相互認証を行った後に、権利書データ106およびコンテンツ鍵データ Kc をEMDサービスセンタ102に登録して権威化する。

また、EMDサービスセンタ102は、6カ月分のキーファイル KF を作成し、これをコンテンツプロバイダ101に送信する。

【0320】

ステップS3：コンテンツプロバイダ101は、図3(A)，(B)に示すコンテンツファイル CF およびその署名データ $SIG_{6,CP}$ と、キーファイル KF およびその署名データ $SIG_{7,CP}$ とを作成し、これらと図3(C)に示す公開鍵証明書データ CER_{cp} およびその署名データ $SIG_{1,ESC}$ とを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、ユーザホームネット

ワーク 103 の SAM105₁ ~ 105₄ に配給する。

オンラインの場合には、コンテンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ 104 がコンテンツプロバイダ 101 からユーザホームネットワーク 103 に配送される。また、オフラインの場合には、ROM 型あるいは RAM 型の記録媒体に記録された状態で、セキュアコンテナ 104 が、コンテンツプロバイダ 101 からユーザホームネットワーク 103 に配送される。

【0321】

ステップ S4：ユーザホームネットワーク 103 の SAM105₁ ~ SAM105₄ は、コンテンツプロバイダ 101 から配給を受けたセキュアコンテナ 104 内の署名データ SIG_{6,CP}, SIG_{7,CP}, SIG_{K1,ESC} を検証して、コンテンツファイル CF およびキーファイル KF の作成者および送信者の正当性を確認した後に、対応する期間のライセンス鍵データ KD₁ ~ KD₆ を用いてキーファイル KF を復号する。

【0322】

ステップ S5：SAM105₁ ~ SAM105₄ において、ユーザによる図 2 に示す操作部 165 の操作に応じたホスト CPU 810 からの内部割り込み S810 に基づいて、購入・利用形態を決定する。

このとき、図 37 に示す利用監視部 186 において、セキュアコンテナ 104 に格納された権利書データ 106 に基づいて、ユーザによるコンテンツファイル CF の購入・利用形態が管理される。

【0323】

ステップ S6：SAM105₁ ~ SAM105₄ の図 37 に示す課金処理部 187 において、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ 108 および利用制御状態データ 166 が生成し、これらを EMD サービスセンタ 102 に送信する。

【0324】

ステップ S7：EMD サービスセンタ 102 は、利用履歴データ 108 に基づ

いて決済処理を行い、決済請求権データ 152 および決済レポートデータ 107 を作成する。EMD サービスセンタ 102 は、決済請求権データ 152 およびその署名データ SIG₉₉ を、図 1 に示すペイメントゲートウェイ 90 を介して、決済機関 91 に送信する。また、EMD サービスセンタ 102 は、決済レポートデータ 107 をコンテンツプロバイダ 101 に送信する。

【0325】

ステップ S8： 決済機関 91 において、署名データ SIG₉₉ の検証を行った後に、決済請求権データ 152 に基づいて、ユーザが支払った金額が、コンテンツプロバイダ 101 の所有者に分配される。

【0326】

以上説明したように、EMD システム 100 では、図 3 に示すフォーマットのセキュアコンテナ 104 をコンテンツプロバイダ 101 からユーザホームネットワーク 103 に配給し、セキュアコンテナ 104 内のキーファイル KF についての処理を SAM105₁ ~ 105₄ 内で行う。

また、キーファイル KF に格納されたコンテンツ鍵データ Kc および権利書データ 106 は、配信鍵データ KD₁ ~ KD₃ を用いて暗号化されており、配信鍵データ KD₁ ~ KD₃ を保持している SAM105₁ ~ 105₄ 内でのみ復号される。そして、SAM105₁ ~ 105₄ では、耐タンパ性を有するモジュールであり、権利書データ 106 に記述されたコンテンツデータ C の取り扱い内容に基づいて、コンテンツデータ C の購入形態および利用形態が決定される。

従って、EMD システム 100 によれば、ユーザホームネットワーク 103 におけるコンテンツデータ C の購入および利用を、コンテンツプロバイダ 101 の関係者が作成した権利書データ 106 の内容に基づいて確実に行わせることができる。

【0327】

また、EMD システム 100 では、コンテンツプロバイダ 101 からユーザホームネットワーク 103 へのコンテンツデータ C の配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ 104 を用いて行うことで、SAM105₁ ~ 105₄ におけるコンテンツデータ C の権利処理を双方の場合におい

て共通化できる。

【0328】

また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁ およびAV機器160₂～160₄ においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0329】

図81は、第1実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。

図81に示すように、マルチプロセッサシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を配送するプロトコルとして例えばTCP/IPおよびXML/SMILが用いられる。

また、ユーザホームネットワーク103のSAM相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク103と103aとの間でセキュアコンテナを転送するプロトコルとして例えば1394シリアルバス・インタフェース上に構築されたXML/SMILが用いられる。また、この場合に、ROM型やRAM型の記録媒体にセキュアコンテナを記録してSAM相互間で配送してもよい。

【0330】

第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄ にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0331】

図82は、本実施形態のEMDシステム300の構成図である。

図82に示すように、EMDシステム300は、コンテンツプロバイダ301

、EMDサービスセンタ 3 0 2、ユーザホームネットワーク 3 0 3、サービスプロバイダ 3 1 0、ペイメントゲートウェイ 9 0 および決済機関 9 1 を有する。

コンテンツプロバイダ 3 0 1、EMDサービスセンタ 3 0 2、SAM 3 0 5₁ ~ 3 0 5₄ およびサービスプロバイダ 3 1 0 は、それぞれ本発明のデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ 3 0 1 は、サービスプロバイダ 3 1 0 に対してコンテンツデータを供給する点を除いて、前述した第 1 実施形態のコンテンツプロバイダ 1 0 1 と同じである。

また、EMDサービスセンタ 3 0 2 は、コンテンツプロバイダ 1 0 1 および SAM 5 0 5₁ ~ 5 0 5₄ に加えて、サービスプロバイダ 3 1 0 に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第 1 実施形態の EMD サービスセンタ 1 0 2 と同じである。

また、ユーザホームネットワーク 3 0 3 は、ネットワーク機器 3 6 0₁ および AV 機器 3 6 0₂ ~ 3 6 0₄ を有している。ネットワーク機器 3 6 0₁ は SAM 3 0 5₁ および CA モジュール 3 1 1 を内蔵しており、AV 機器 3 6 0₂ ~ 3 6 0₄ はそれぞれ SAM 3 0 5₂ ~ 3 0 5₄ を内蔵している。

ここで、SAM 3 0 5₁ ~ 3 0 5₄ は、サービスプロバイダ 3 1 0 からセキュアコンテナ 3 0 4 の配給を受ける点と、コンテンツプロバイダ 3 0 1 に加えてサービスプロバイダ 3 1 0 についての署名データの検証処理および SP 用購入履歴データ（データ配給装置用購入履歴データ）3 0 9 の作成を行なう点とを除いて、前述した第 1 実施形態の SAM 1 0 5₁ ~ 1 0 5₄ と同じである。

【0 3 3 2】

先ず、EMD システム 3 0 0 の概要について説明する。

EMD システム 3 0 0 では、コンテンツプロバイダ 3 0 1 は、自らが提供しようとするコンテンツのコンテンツデータ C の使用許諾条件などの権利内容を示す前述した第 1 実施形態と同様の権利書 (UCP: Usage Control Policy) データ 1 0 6 およびコンテンツ鍵データ K c を、高い信頼性のある権威機関である EMD サービスセンタ 3 0 2 に送信する。権利書データ 1 0 6 およびコンテンツ鍵データ K c は、EMD サービスセンタ 3 0 2 に登録されて権威化（認証）される。

【0333】

また、コンテンツプロバイダ301は、コンテンツ鍵データK_cでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から、各コンテンツファイルCFについて、それぞれ6か月分のキーファイルKFを受信する。

当該キーファイルKF内には、当該キーファイルKFの改竄の有無、当該キーファイルKFの作成者および送信者の正当性を検証するための署名データが格納されている。

そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納した図3に示すセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ310に供給する。

また、セキュアコンテナ104に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0334】

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104の作成者および送信者の確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格（SRP）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（PT：本発明の価格データ）312を作成する。

そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対しての自らの秘密鍵データK_{SP,S}による署名データとを格納したセキュアコンテナ304を作成する。

このとき、キーファイルKFは、ライセンス鍵データKD₁～KD₆によって

暗号化されており、サービスプロバイダ 310 は当該ライセンス鍵データ $KD_1 \sim KD_6$ を保持していないため、サービスプロバイダ 310 はキーファイル KF の中身を見たり、書き換えたりすることはできない。

また、EMD サービスセンタ 302 は、プライスタグデータ 312 を登録して権威化する。

【0335】

サービスプロバイダ 310 は、オンラインおよび／またはオフラインでセキュアコンテナ 304 をユーザホームネットワーク 303 に配給する。

このとき、オフラインの場合には、セキュアコンテナ 304 は ROM 型の記録媒体などに記録されて $SAM305_1 \sim 305_4$ にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ 310 と CA モジュール 311 との間で相互認証を行い、セキュアコンテナ 304 をサービスプロバイダ 310 においてセッション鍵データ K_{SES} を用いた暗号化して送信し、CA モジュール 311 において受信したセキュアコンテナ 304 をセッション鍵データ K_{SES} を用いて復号した後に、 $SAM305_1 \sim 305_4$ に転送する。

この場合に、コンテンツプロバイダ 301 からユーザホームネットワーク 303 にセキュアコンテナ 304 を送信する通信プロトコルとして、デジタル放送であれば MHEG (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットであれば XML / SMIL / HTML (Hyper Text Markup Language) が用いられ、これらの通信プロトコル内に、セキュアコンテナ 304 が、当該通信プロトコル (符号化方式など) に依存しない形式でトンネリングして埋め込まれる。

従って、通信プロトコルとセキュアコンテナ 304 との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ 304 のフォーマットを柔軟に設定できる。

【0336】

次に、 $SAM305_1 \sim 305_4$ において、セキュアコンテナ 304 内に格納された署名データを検証して、セキュアコンテナ 304 に格納されたコンテンツファイル CF およびキーファイル KF の作成者および送信者の正当性を確認する

。そして、SAM 3 0 5₁ ~ 3 0 5₄ において、当該正当性が確認されると、EMD サービスセンタ 3 0 2 から配給された対応する期間のライセンス鍵データ K D₁ ~ K D₃ を用いてキーファイル K F を復号する。

SAM 3 0 5₁ ~ 3 0 5₄ に供給されたセキュアコンテナ 3 0 4 は、ネットワーク機器 3 6 0₁ および A V 機器 3 6 0₂ ~ 3 6 0₄ において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM 3 0 5₁ ~ 3 0 5₄ は、上述したセキュアコンテナ 3 0 4 の購入・利用の履歴を利用履歴 (Usage Log) データ 3 0 8 として記録する。

利用履歴データ (履歴データまたは管理装置用履歴データ) 3 0 8 は、例えば、EMD サービスセンタ 3 0 2 からの要求に応じて、ユーザホームネットワーク 3 0 3 から EMD サービスセンタ 3 0 2 に送信される。

また、SAM 3 0 5₁ ~ 3 0 5₄ は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御データ (U C S : Usage control state Data) 1 6 6 を EMD サービスセンタ 3 0 2 に送信する。

【 0 3 3 7 】

EMD サービスセンタ 3 0 2 は、利用履歴データ 3 0 8 に基づいて、コンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 の各々について、課金内容を決定 (計算) し、その結果に基づいて、ペイメントゲートウェイ 9 0 を介して銀行などの決済機関 9 1 に決済を行なう。これにより、ユーザホームネットワーク 1 0 3 のユーザが支払った金銭が、EMD サービスセンタ 1 0 2 による決済処理によって、コンテンツプロバイダ 1 0 1 およびサービスプロバイダ 3 1 0 に分配される。

【 0 3 3 8 】

本実施形態では、EMD サービスセンタ 3 0 2 は、認証機能、鍵データ管理機能および権利処理 (利益分配) 機能を有している。

すなわち、EMD サービスセンタ 3 0 2 は、中立の立場にある最高の権威機関であるルート認証局 9 2 に対してのセカンド認証局 (Second Certificate Authority) としての役割を果たし、コンテンツプロバイダ 3 0 1、サービスプロバイダ

310 および SAM305₁ ~ 305₄ において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMD サービスセンタ 302 の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ 301 の権利書データ 106、コンテンツ鍵データ Kc およびサービスプロバイダ 310 のプライスタグデータ 312 を登録して権威化することも、EMD サービスセンタ 302 の認証機能によるものである。

また、EMD サービスセンタ 302 は、例えば、ライセンス鍵データ KD₁ ~ KD₆ などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMD サービスセンタ 302 は、コンテンツプロバイダ 301 が登録した権利書データ 106 と SAM305₁ ~ SAM305₄ から入力した利用履歴データ 308 とサービスプロバイダ 310 が登録したプライスタグデータ 312 とに基づいて、ユーザホームネットワーク 303 のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ 301 およびサービスプロバイダ 310 に分配して支払う権利処理（利益分配）機能を有する。

【0339】

以下、コンテンツプロバイダ 301 の各構成要素について詳細に説明する。

〔コンテンツプロバイダ 301〕

コンテンツプロバイダ 301 は、図 3 に示すセキュアコンテナ 104 をオンラインあるいはオフラインでサービスプロバイダ 310 に提供する点を除いて、前述した第 1 実施形態のコンテンツプロバイダ 101 と同じである。

すなわち、コンテンツプロバイダ 301 は、前述した図 17 ~ 図 19 に示す手順でセキュアコンテナ 104 を作成し、セキュアコンテナ 104 を、コンテンツプロバイダ用商品配送プロトコルに挿入する。

そして、サービスプロバイダ 310 が、ダウンロードを行って、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ 104 を取り出す。

【0340】

〔サービスプロバイダ 310〕

サービスプロバイダ 310 は、コンテンツプロバイダ 301 から提供を受けたセキュアコンテナ 104 内のコンテンツファイル CF およびキーファイル KF と、自らが生成したプライスタグデータ 312 とを格納したセキュアコンテナ 304 を作成し、ユーザホームネットワーク 303 のネットワーク機器 360₁ および AV 機器 360₂ ~ 360₄ にセキュアコンテナ 304 をオンラインおよび／またはオフラインで配給する。

サービスプロバイダ 310 によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0341】

サービスプロバイダ 310 は、コンテンツプロバイダ 301 からセキュアコンテナ 104 の提供を受けると、以下に示す処理を行ってセキュアコンテナ 304 を作成する。

以下、コンテンツプロバイダ 301 から供給を受けたセキュアコンテナ 104 からセキュアコンテナ 304 を作成し、これをユーザホームネットワーク 303 に配給する際のサービスプロバイダ 310 内での処理の流れを図 83 を参照しながら説明する。

図 83 は、サービスプロバイダ 310 からユーザホームネットワーク 303 にセキュアコンテナ 304 を配給する処理を説明するためのフローチャートである。

<ステップ S83-1>

サービスプロバイダ 310 は、オンラインおよび／またはオフラインで、コンテンツプロバイダ 301 から図 3 に示すセキュアコンテナ 104 の供給を受け、これを格納する。

このとき、オンラインの場合には、コンテンツプロバイダ 301 とサービスプ

ロバイダ 310 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて、セキュアコンテナ 104 を復号する。

<ステップ S83-2>

サービスプロバイダ 310 は、セキュアコンテナ 104 の図 3 (C) に示す署名データ $SIG_{1,ESC}$ を、EMD サービスセンタ 302 の公開鍵データ $K_{ESC,P}$ を用いて検証し、その正当性が認められた後に、図 3 (C) に示す公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP,P}$ を取り出す。

次に、サービスプロバイダ 310 は、当該取り出した公開鍵データ $K_{CP,P}$ を用いて、セキュアコンテナ 104 の図 3 (A), (B) に示す署名データ $SIG_{6,CP}$, $SIG_{7,CP}$ の検証、すなわちコンテンツファイル CF の作成者および送信者と、キーファイル KF の送信者との正当性の検証を行う。

また、サービスプロバイダ 310 は、公開鍵データ $K_{ESC,P}$ を用いて、図 3 (B) に示すキーファイル KF に格納された署名データ $SIG_{K1,ESC}$ の検証、すなわちキーファイル KF の作成者の正当性の検証を行う。このとき、署名データ $SIG_{K1,ESC}$ の検証は、キーファイル KF が EMD サービスセンタ 302 に登録されているか否かの検証も兼ねている。

【0342】

<ステップ S83-3>

サービスプロバイダ 310 は、例えばコンテンツプロバイダ 301 からオフラインで通知されたコンテンツプロバイダ 301 が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ 312 を作成する。

また、サービスプロバイダ 310 は、コンテンツファイル CF、キーファイル KF およびプライスタグデータ 312 のハッシュ値をとり、サービスプロバイダ 310 の秘密鍵データ $K_{SP,P}$ を用いて、署名データ $SIG_{62,SP}$, $SIG_{63,SP}$, $SIG_{64,SP}$ を作成する。

ここで、署名データ $SIG_{62,SP}$ はコンテンツファイル CF の送信者の正当性を検証するために用いられ、署名データ $SIG_{63,SP}$ はキーファイル KF の送信者の正当性を検証するために用いられ、署名データ $SIG_{64,SP}$ はプライスタグ

データ 3 1 2 の作成者および送信者の正当性を検証するために用いられる。

【0 3 4 3】

次に、サービスプロバイダ 3 1 0 は、図 8 4 (A) ～ (D) に示すように、コンテンツファイル C F およびその署名データ S I G_{6,CP}, S I G_{62,SP} と、キーファイル K F およびその署名データ S I G_{7,CP}, S I G_{63,ESC} と、プライスタグデータ 3 1 2 およびその署名データ S I G_{64,SP} と、公開鍵証明書データ C E R_{SP} およびその署名データ S I G_{61,ESC} と、公開鍵証明書データ C E R_{CP} およびその署名データ S I G_{1,ESC} とを格納したセキュアコンテナ 3 0 4 を作成し、セキュアコンテナデータベースに格納する。

セキュアコンテナデータベースに格納されたセキュアコンテナ 3 0 4 は、例えば、コンテンツ I D などを用いてサービスプロバイダ 3 1 0 によって一元的に管理される。

なお、図 8 4 (A) は、コンテンツデータ C を伸長する A V 圧縮伸長用装置として、D S P (Digital Signal Processor) を用いた場合のコンテンツファイル C F の構成である。当該 D S P では、セキュアコンテナ 3 0 4 内の A / V 伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ 1 0 4 内のコンテンツデータ C の伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ 3 0 1 は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。

A V 圧縮伸長用装置として A / V 伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイル C F 内に A / V 伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【0 3 4 4】

<ステップ S 8 3－4>

サービスプロバイダ 3 1 0 は、ユーザホームネットワーク 3 0 3 からの要求に応じたセキュアコンテナ 3 0 4 をセキュアコンテナデータベースから読み出す。

このとき、セキュアコンテナ 3 0 4 は、複数のコンテンツファイル C F と、それらにそれぞれ対応した複数のキーファイル K F とを格納した複合コンテナであ

ってもよい。例えば、単数のセキュアコンテナ 304 内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイル CF を単数のセキュアコンテナ 304 に格納してもよい。これらの複数のコンテンツファイル CF などは、ディレクトリー構造でセキュアコンテナ 304 内に格納してもよい。

【0345】

また、セキュアコンテナ 304 は、デジタル放送で送信される場合には、MHEG (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットで送信される場合には XML / SMIL / HTML (Hyper TextMarkup Language) プロトコルが用いられる。

このとき、セキュアコンテナ 304 内のコンテンツファイル CF およびキーファイル KF などは、MHEG および HTML のプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ 310 とユーザホームネットワーク 303 との間で採用される通信プロトコル内の所定の階層に格納される。

【0346】

例えば、セキュアコンテナ 304 をデジタル放送で送信する場合には、図 85 に示すように、コンテンツファイル CF が、MHEG オブジェクト (Object) 内の MHEG コンテンツデータとして格納される。

また、MHEG オブジェクトは、トランスポート層プロトコルにおいて、動画である場合には PES (Packetized Elementary Stream) - Video に格納され、音声である場合には PES - Audio に格納され、静止画である場合には Private Data に格納される。

また、図 86 に示すように、キーファイル KF、プライスタグデータ 312 および公開鍵証明書データ CER_{CP} 、 CER_{SP} は、トランスポート層プロトコルの TS Packet 内の ECM (Entitlement Control Message) に格納される。

ここで、コンテンツファイル CF、キーファイル KF、プライスタグデータ 312 および公開鍵証明書データ CER_{CP} 、 CER_{SP} は、コンテンツファイル CF のヘッダ内のディレクトリー構造データ DSD_1 によって相互間のリンクが確立されている。

【0 3 4 7】

次に、サービスプロバイダ 3 1 0 は、セキュアコンテナ 3 0 4 を、オフラインおよび／またはオンラインでユーザホームネットワーク 3 0 3 に供給する。

サービスプロバイダ 3 1 0 は、セキュアコンテナ 3 0 4 をオンラインでユーザホームネットワーク 3 0 3 のネットワーク機器 3 6 0₁ に配信する場合には、相互認証後に、セッション鍵データ K_{SES} を用いてセキュアコンテナ 3 0 4 を暗号化した後に、ネットワークを介してネットワーク機器 3 6 0₁ に配信する。

【0 3 4 8】

なお、サービスプロバイダ 3 1 0 は、セキュアコンテナ 3 0 4 を例えば衛星などを介して放送する場合には、セキュアコンテナ 3 0 4 をスクランブル鍵データ K_{SCR} を用いて暗号化する。また、スクランブル鍵データ K_{SCR} をワーク鍵データ K_W を暗号化し、ワーク鍵データ K_W をマスタ鍵データ K_M を用いて暗号化する。

そして、サービスプロバイダ 3 1 0 は、セキュアコンテナ 3 0 4 と共に、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を、衛星を介してユーザホームネットワーク 3 0 3 に送信する。

また、例えば、マスタ鍵データ K_M を、ICカードなどに記憶してオフラインでユーザホームネットワーク 3 0 3 に配給する。

【0 3 4 9】

また、サービスプロバイダ 3 1 0 は、ユーザホームネットワーク 3 0 3 から、当該サービスプロバイダ 3 1 0 が配給したコンテンツデータ C についての SP 用購入履歴データ 3 0 9 を受信すると、これを格納する。

サービスプロバイダ 3 1 0 は、将来のサービス内容を決定する際に、SP 用購入履歴データ 3 0 9 を参照する。また、サービスプロバイダ 3 1 0 は、SP 用購入履歴データ 3 0 9 に基づいて、当該 SP 用購入履歴データ 3 0 9 を送信した SAM 3 0 5₁ ~ 3 0 5₄ のユーザの嗜好を分析してユーザ嗜好フィルタデータ 9 0 0 を生成し、これをユーザホームネットワーク 3 0 3 の CA モジュール 3 1 1 に送信する。

【0350】

また、サービスプロバイダ310の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP_IDを得ている。

【0351】

また、サービスプロバイダ310は、EMDサービスセンタ302にプライスタグデータ312を登録して権威化してゐる。

【0352】

[EMDサービスセンタ302]

EMDサービスセンタ302は、前述したように、認証局(CA:Certificate Authority)、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。

図87は、EMDサービスセンタ302の主な機能を示す図である。

図87に示すように、EMDサービスセンタ302は、主に、ライセンス鍵データをコンテンツプロバイダ301およびSAM305₁～305₄に供給する処理と、公開鍵証明書データCER_{CP}、CER_{SP}、CER_{SAM1}～CER_{SAM4}の発行処理と、キーファイルKFの発行処理、利用履歴データ308に基づいた決済処理(利益分配処理)とを行う。

ここで、ライセンス鍵データの供給処理と、公開鍵証明書データCER_{CP}、CER_{SAM1}～CER_{SAM4}の発行処理と、キーファイルKFの生成処理とは、第1実施形態のEMDサービスセンタ102と同じである。

【0353】

EMDサービスセンタ302は、EMDサービスセンタ102とは異なり、さらにサービスプロバイダ310の公開鍵証明書データCER_{SP}の発行処理を行う。

また、EMDサービスセンタ302は、利用履歴データ308に基づいて、SAM305₁～305₄におけるコンテンツデータCの購入によって支払われた利益をコンテンツプロバイダ301およびサービスプロバイダ310の関係者に分配する利益分配処理を行う。

ここで、利用履歴データ 308 の内容は、例えば図 21 に示される。

【0354】

また、EMD サービスセンタ 302 は、利用履歴データ 308 に基づいて、当該利用履歴データ 308 を送信した SAM 305₁ ~ 305₄ のユーザの嗜好に応じたコンテンツデータ C を選択するためのユーザ嗜好フィルタデータ 903 を生成し、ユーザ嗜好フィルタデータ 903 を SAM 管理部 149 を介して、当該利用履歴データ 308 を送信した SAM 305₁ ~ 305₄ に送信する。

【0355】

[ユーザホームネットワーク 303]

ユーザホームネットワーク 303 は、図 82 に示すように、ネットワーク機器 360₁ および A/V 機器 360₂ ~ 360₄ を有している。

ネットワーク機器 360₁ は、CA モジュール 311 および SAM 305₁ を内蔵している。また、A/V 機器 360₂ ~ 360₄ は、それぞれ SAM 305₂ ~ 305₄ を内蔵している。

SAM 305₁ ~ 305₄ の相互間は、例えば、1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。

なお、A/V 機器 360₂ ~ 360₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 360₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク 303 は、ネットワーク機能を有していない A/V 機器のみを有していてもよい。

【0356】

以下、ネットワーク機器 360₁ について説明する。

図 88 は、ネットワーク機器 360₁ の構成図である。

図 88 に示すように、ネットワーク機器 360₁ は、通信モジュール 162、CA モジュール 311、復号モジュール 905、SAM 305₁、A/V 圧縮・伸長用 SAM 163、操作部 165、ダウンロードメモリ 167、再生モジュール 169、外部メモリ 201 およびホスト CPU 810 を有する。

図 88 において、図 22 と同一符号を付した構成要素は、第 1 実施形態で説明

した同一符号の構成要素と同じである。

【0357】

通信モジュール162は、サービスプロバイダ310との間の通信処理を行なう。

具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などで受信したセキュアコンテンツ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310から電話回線などを介して受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

【0358】

図89は、CAモジュール311および復号モジュール905の機能ブロック図である。

図89に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。

相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との間で相互認証を行ってセッション鍵データ K_{SES} を生成し、これを暗号化・復号部908に出力する。

【0359】

記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データ K_M を記憶する。

【0360】

暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力し、記憶部907から読み出したマスタ鍵データ K_M を用いてワーク鍵データ K_W を復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データ K_W

を用いてスクランブル鍵データ K_{SCR} を復号し、当該復号したスクランブル鍵データ K_{SCR} を復号部 910 に出力する。

また、暗号化・復号部 908 は、電話回線などを介して通信モジュール 162 がサービスプロバイダ 310 から受信したユーザ嗜好フィルタデータ 900 を、相互認証部 906 からのセッション鍵データ K_{SES} を用いて復号して復号モジュール 905 のセキュアコンテナ選択部 911 に出力する。

また、暗号化・復号部 908 は、SP 用購入履歴データ生成部 909 から入力した SP 用購入履歴データ 309 を、相互認証部 906 からのセッション鍵データ K_{SES} を用いて復号して通信モジュール 162 を介してサービスプロバイダ 310 に送信する。

【0361】

SP 用購入履歴データ生成部 909 は、図 88 に示す購入・利用形態決定操作部 165 を用いてユーザによるコンテンツデータ C の購入操作に応じた操作信号 $S165$ 、または $SAM305_1$ からの利用制御データ 166 に基づいて、サービスプロバイダ 310 に固有のコンテンツデータ C の購入履歴を示す SP 用購入履歴データ 309 を生成し、これを暗号化・復号部 908 に出力する。

SP 用購入履歴データ 309 は、例えば、サービスプロバイダ 310 が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0362】

なお、CA モジュール 311 は、サービスプロバイダ 310 が課金機能を有している場合には、サービスプロバイダ 310 の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CA モジュール 311 は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ 310 に送信する。

【0363】

復号モジュール 905 は、復号部 910 およびセキュアコンテナ選択部 911 を有する。

復号部 910 は、通信モジュール 162 から、それぞれ暗号化されたセキュア

コンテナ 304、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力する。

そして、復号部 910 は、暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を CA モジュール 311 の暗号化・復号部 908 に出力し、暗号化・復号部 908 から復号されたスクランブル鍵データ K_{SCR} を入力する。

そして、復号部 910 は、暗号化されたセキュアコンテナ 304 を、スクランブル鍵データ K_{SCR} を用いて復号した後に、セキュアコンテナ選択部 911 に出力する。

【0364】

なお、セキュアコンテナ 304 が、MPEG2 Transport Stream 方式でサービスプロバイダ 310 から送信される場合には、例えば、復号部 910 は、TS Packet 内の ECM (Entitlement Control Message) からスクランブル鍵データ K_{SCR} を取り出し、EMM (Entitlement Management Message) からワーク鍵データ K_W を取り出す。

ECM には、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMM は、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【0365】

セキュアコンテナ選択部 911 は、復号部 910 から入力したセキュアコンテナ 304 を、CA モジュール 311 から入力したユーザ嗜好フィルタデータ 900 を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ 304 を選択して SAM 305₁ に出力する。

【0366】

次に、SAM 305₁ について説明する。

なお、SAM 305₁ は、サービスプロバイダ 310 についての署名検証処理を行なうなど、コンテンツプロバイダ 301 に加えてサービスプロバイダ 310 に関しての処理を行う点を除いて、図 22～図 72 などを用いて前述した第 1 実施形態の SAM 105₁ と基本的に行なう機能および構造を有している。

SAM305₁～305₄ は、コンテンツ単位の課金処理を行うモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0367】

また、図63に示す構成はユーザホームネットワーク303内の機器においても適用可能である。また、図68～図79を用いて説明した権利処理用のSAM、メディアSAM133、AV圧縮・伸長用SAM163およびメディア・ドラブSAM260の構成は、ユーザホームネットワーク303内の機器で用いられる各種のSAMにも適用される。

また、SAM305₂～305₄ は、SAM305₁ と基本的に同じ機能を有

【0368】

以下、SAM305₁ の機能について詳細に説明する。

図90は、SAM305₁ の機能の構成図である。

なお、図90には、サービスプロバイダ310からセキュアコンテナ304を入力する際の処理に関連するデータの流れが示されている。

図90に示すように、SAM305₁ は、相互認証部170、暗号化・復号部171、172、173、ダウンロードメモリ管理部182、AV圧縮・伸長用SAM管理部184、EMDサービスセンタ管理部185、利用監視部186、SAM管理部190、記憶部192、メディアSAM管理部197、作業用メモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部589、外部メモリ管理部811およびCPU1100を有する。

なお、図90に示すSAM305₁ の所定の機能は、SAM105₁ の場合と同様に、CPUにおいて秘密プログラムを実行することによって実現される。

図90において、図30等と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと同じである。

【0369】

また、図88に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。

また、作業用メモリ200には、図91に示すように、コンテンツ鍵データK

c、権利書データ (UCP) 106、記憶部 192 のロック鍵データ K_{LOC} 、コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} 、サービスプロバイダ 310 の公開鍵証明書データ CER_{SP} 、利用制御データ (UCS) 366、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ およびプライスタグデータ 312 などが記憶される。

【0370】

以下、SAM305₁ の機能ブロックのうち、図90において新たに符号を付した機能ブロックについて説明する。

署名処理部 589 は、記憶部 192 あるいは作業用メモリ 200 から読み出した EMD サービスセンタ 302 の公開鍵データ $K_{ESC,P}$ 、コンテンツプロバイダ 301 の公開鍵データ $K_{cp,p}$ およびサービスプロバイダ 310 の公開鍵データ $K_{SP,P}$ を用いて、セキュアコンテナ 304 内の署名データの検証を行なう。

【0371】

課金処理部 587 は、図92に示すように、ユーザによる購入形態決定操作に応じた内部割り込み S810 を CPU1100 がホスト CPU810 から受けると、CPU1100 からの制御によって、作業用メモリ 200 から読み出されたプライスタグデータ 312 に基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

なお、プライスタグデータ 312 は、ユーザがコンテンツデータの購入形態等を決定する際に、所定の出力手段を介して SAM305₁ の外部に出力され、コンテンツデータの販売価格をユーザに表示等するために用いられる。

課金処理部 587 による課金処理は、利用監視部 186 の監視の下、権利書データ 106 が示す使用許諾条件などの権利内容および利用制御データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0372】

また、課金処理部 587 は、課金処理において、利用履歴データ 308 を生成あるいは更新し、これを外部メモリ管理部 811 を介して外部メモリ 201 に書き込む。

ここで、利用履歴データ 3 0 8 は、第 1 実施形態の利用履歴データ 1 0 8 と同様に、EMD サービスセンタ 3 0 2 において、セキュアコンテナ 3 0 4 に関連したライセンス料の支払いを決定する際に用いられる。

【 0 3 7 3 】

また、課金処理部 5 8 7 は、ユーザによる購入形態決定操作に応じた CPU 1 1 0 0 の制御に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御 (UCS: Usage Control Status) データ 1 6 6 を生成し、これを作業用メモリ 2 0 0 に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御データ 1 6 6 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ 1 6 6 には、コンテンツの ID、購入形態、買い切り価格、当該コンテンツの購入が行なわれた SAM の SAM__ID、購入を行なったユーザの USER__ID などが記述されている。

【 0 3 7 4 】

なお、決定された購入形態が再生課金である場合には、例えば、SAM 3 0 5₁ からサービスプロバイダ 3 1 0 に利用制御データ 1 6 6 をリアルタイムに送信し、サービスプロバイダ 3 1 0 が EMD サービスセンタ 3 0 2 に、利用履歴データ 3 0 8 を SAM 1 0 5₁ に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御データ 1 6 6 が、サービスプロバイダ 3 1 0 および EMD サービスセンタ 3 0 2 にリアルタイムに送信される。

【 0 3 7 5 】

また、SAM 3 0 5₁ では、図 9 0 に示すように、EMD サービスセンタ管理部 1 8 5 を介して EMD サービスセンタ 3 0 2 から受信したユーザ嗜好フィルタデータ 9 0 3 が、サービスプロバイダ管理部 5 8 0 に出力される。そして、サー

ビスプロバイダ管理部 580 において、図 88 に示す復号モジュール 905 から入力したセキュアコンテナ 304 のうち、ユーザ嗜好フィルタデータ 903 に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ 304 が選択され、当該選択されたセキュアコンテナ 304 がダウンロードメモリ管理部 182 に出力される。これにより、SAM305₁ において、当該 SAM305₁ のユーザが契約している全てのサービスプロバイダ 310 を対象として、当該ユーザによるコンテンツデータ C の購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータ C の選択処理が可能になる。

【0376】

以下、SAM305₁ 内での処理の流れを説明する。

<ライセンス鍵データの受信時の処理>

EMD サービスセンタ 302 から受信したライセンス鍵データ KD₁ ~ KD₃ を記憶部 192 に格納する際の SAM305₁ 内での処理の流れは、図 35 を用いて前述した第 1 実施形態の SAM105₁ の場合と同様である。

【0377】

<セキュアコンテナ 304 をサービスプロバイダ 310 から入力した時の処理>

次に、セキュアコンテナ 304 をサービスプロバイダ 310 から入力する際の SAM305₁ 内での処理の流れを図 93 を参照しながら説明する。

なお、以下に示す例では、SAM105₁ において、セキュアコンテナ 104 を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ 104 の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

【0378】

ステップ S93-0：図 90 に示す SAM305₁ の CPU1100 は、ホスト CPU810 から、セキュアコンテナの入力処理を行うことを指示する内部割り込み S810 を受ける。

ステップ S93-1：図 90 に示す SAM305₁ の相互認証部 170 とサービスプロバイダ 310 との間で相互認証を行なう。

ステップ S93-2 : SAM305₁ の相互認証部 170 とダウンロードメモリ 167 のメディア SAM167a との間で相互認証を行なう。

【0379】

ステップ S93-3 : サービスプロバイダ 310 から受信したセキュアコンテナ 304 を、ダウンロードメモリ 167 に書き込む。

このとき、ステップ S93-2 で得られたセッション鍵データを用いて、相互認証部 170 におけるセキュアコンテナ 304 の暗号化と、メディア SAM167a におけるセキュアコンテナ 304 の復号とを行なう。

ステップ S93-4 : SAM305₁ は、ステップ S93-1 で得られたセッション鍵データを用いて、セキュアコンテナ 304 の復号を行なう。

【0380】

ステップ S93-5 : 署名処理部 589 は、図 84 (D) に示す署名データ SIG_{61,ESC} の検証を行なった後に、図 84 (D) に示す公開鍵証明書データ CER_{SP} 内に格納されたサービスプロバイダ 310 の公開鍵データ K_{SP,P} を用いて、署名データ SIG_{62,SP} , SIG_{63,SP} , SIG_{64,SP} の正当性を検証する。

このとき、署名データ SIG_{62,SP} が正当であると検証されたときに、コンテンツファイル CF の送信者の正当性が確認される。署名データ SIG_{63,SP} が正当であると検証されたときに、キーファイル KF の送信者の正当性が確認される。署名データ SIG_{64,SP} が正当であると検証されたときに、プライスタグデータ 312 の作成者および送信者の正当性が確認される。

【0381】

ステップ S93-6 : 署名処理部 589 は、図 84 (D) に示す署名データ SIG_{1,ESC} の検証を行なった後に、図 84 (C) に示す公開鍵証明書データ CER_{CP} 内に格納されたコンテンツプロバイダ 301 の公開鍵データ K_{CP,P} を用いて、署名データ SIG_{6,CP} , SIG_{7,CP} の正当性を検証する。

このとき、署名データ SIG_{6,CP} が正当であると検証されたときに、コンテンツファイル CF の作成者および送信者の正当性が確認される。

また、署名データ SIG_{7,CP} が正当であると検証されたときに、キーファイル KF の送信者の正当性が確認される。

【0382】

ステップS93-7：署名処理部589は、記憶部192から読み出した公開鍵データ $K_{ESC,P}$ を用いて、図84（B）に示すキーファイルKF内の署名データ $SIG_{K1,ESC}$ の正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。

【0383】

ステップS93-8：暗号化・復号部172は、記憶部192から読み出した対応する期間のライセンス鍵データ $KD_1 \sim KD_3$ を用いて、図84（B）に示すキーファイルKF内のコンテンツ鍵データ Kc 、権利書データ106およびSAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ を復号し、これらを作業用メモリ200に書き込む。

【0384】

ステップS93-9：CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。

なお、CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0385】

＜ダウンロードしたセキュアコンテナの購入形態決定処理＞

ダウンロードしたセキュアコンテナの購入形態決定処理は、基本的に、第1実施形態において、図38を用いて前述したSAM105₁の場合と同じである。

当該購入形態決定処理により、後述する図97（C）に示すキーファイルKF₁が作業用メモリ200およびダウンロードメモリ管理部182を介してダウンロードメモリ167に記憶される。

【0386】

＜コンテンツデータの再生処理＞

ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCの再生処理は、基本的に、第1実施形態において、図40を用いて

説明した SAM 1 0 5₁ の処理と同じである。

【 0 3 8 7 】

＜一の機器の利用制御データ（USC） 1 6 6 を使用して他の機器で再購入を行う場合の処理＞

先ず、図 9 4 に示すように、例えば、ネットワーク機器 3 6 0₁ のダウンロードメモリ 1 6 7 にダウンロードされたコンテンツファイル CF の購入形態を前述したように決定した後に、当該コンテンツファイル CF を格納した新たなセキュアコンテナ 3 0 4 x を生成し、バス 1 9 1 を介して、AV 機器 3 6 0₂ の SAM 3 0 5₂ にセキュアコンテナ 3 0 4 x を転送するまでの SAM 1 0 5₁ 内での処理の流れを図 9 5 および図 9 6 を参照しながら説明する。

【 0 3 8 8 】

図 9 6 は、当該処理のフローチャートである。

図 9 6 に示す処理を行う前提として、前述した購入処理によって、SAM 3 0 5₁ の作業用メモリ 2 0 0 には図 9 7（C）に示すキーファイル KF₁ およびそのハッシュ値 H_{K1} が記憶されている。

ステップ S 9 6 - 1 : ユーザは図 8 8 および図 9 4 に示すに操作部 1 6 5 を操作し、購入形態を既に決定したセキュアコンテナを SAM 3 0 5₂ に転送することを示す内部割り込み S 8 1 0 がホスト CPU 8 1 0 から図 9 5 に示す CPU 1 1 0 0 に出される。

課金処理部 5 8 7 は、CPU 1 1 0 0 の制御に基づいて、決定された購入形態に応じて、外部メモリ 2 0 1 に記憶されている利用履歴データ 3 0 8 を更新する。

【 0 3 8 9 】

ステップ S 9 6 - 2 : SAM 3 0 5₁ は、第 1 実施形態で前述した SAM 登録リストを検証し、セキュアコンテナの転送先の SAM 3 0 5₂ が正規に登録されている SAM であるか否かを検証し、正規に登録されていると判断した場合にステップ S 9 6 - 3 以降の処理を行う。

また、SAM 1 0 5₁ は、SAM 1 0 5₂ がホームネットワーク内の SAM であるか否かの検証も行う。

【0390】

ステップ S 9 6 - 3 : 相互認証部 1 7 0 は、SAM 3 0 5₂ との間で相互認証を行って得たセッション鍵データ K_{SES} を共有する。

【0391】

ステップ S 9 6 - 4 : SAM 管理部 1 9 0 は、ダウンロードメモリ 2 1 1 から図 8 4 (A) に示すコンテンツファイル CF および署名データ S I G_{6,CP}, S I G_{62,SP} を読み出し、これについての SAM 1 0 5₁ の秘密鍵データ K_{SAM1} を用いた署名データ S I G_{41,SAM1} を署名処理部 1 8 9 に作成させる。

【0392】

ステップ S 9 6 - 5 : SAM 管理部 1 9 0 は、ダウンロードメモリ 2 1 1 から図 8 4 (B) に示すキーファイル KF および署名データ S I G_{7,CP}, S I G_{63,SP} を読み出し、これについての SAM 3 0 5₁ の秘密鍵データ K_{SAM1} を用いた署名データ S I G_{42,SAM1} を署名処理部 5 8 9 に作成させる。

【0393】

ステップ S 9 6 - 6 : SAM 管理部 1 9 0 は、図 9 7 に示すセキュアコンテナ 3 0 4 x を作成する。

ステップ S 9 6 - 7 : 暗号化・復号部 1 7 1 において、ステップ S 9 6 - 3 で得たセッション鍵データ K_{SES} を用いて、図 9 7 に示すセキュアコンテナ 3 0 4 x が暗号化される。

【0394】

ステップ S 9 6 - 8 : SAM 管理部 1 9 0 は、セキュアコンテナ 3 0 4 x を図 9 4 に示す AV 機器 3 6 0₂ の SAM 3 0 5₂ に出力する。

このとき、SAM 3 0 5₁ と SAM 3 0 5₂ との間の相互認証と並行して、I E E 1 3 9 4 シリアルバスであるバス 1 9 1 の相互認証が行われる。

【0395】

ステップ S 9 6 - 9 : CPU 1 1 0 0 は、上述したセキュアコンテナの転送処理が適切に行われたか否かを、外部割り込みでホスト CPU 8 1 0 に通知する。

なお、CPU 1 1 0 0 は、上述したセキュアコンテナの転送処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU 8

1 0 がポーリングによって当該フラグを読んでもよい。

【0 3 9 6】

以下、図 9 4 に示すように、SAM 3 0 5₁ から入力した図 9 7 に示すセキュアコンテナ 3 0 4 x を、RAM 型などの記録媒体（メディア）1 3 0₄ に書き込む際の SAM 3 0 5₂ 内での処理の流れを図 9 8、図 9 9 および図 1 0 0 を参照して説明する。

図 9 9 および図 1 0 0 は、当該処理を示すフローチャートである。

ここで、RAM 型の記録媒体 1 3 0₄ は、例えば、セキュアでない RAM 領域 1 3 4、メディア SAM 1 3 3 およびセキュア RAM 領域 1 3 2 を有している。

【0 3 9 7】

ステップ S 9 9－0：図 9 8 に示す SAM 3 0 5₂ の CPU 1 1 0 0 は、ホスト CPU 8 1 0 から、入力したセキュアコンテナを購入形態を決定した後に記録媒体に記録することを指示する内部割り込み S 8 1 0 を受ける。

【0 3 9 8】

ステップ S 9 9－1：SAM 3 0 5₂ は、SAM 登録リストを検証し、セキュアコンテナの転送元の SAM 3 0 5₁ が正規に登録されている SAM であるか否かを検証し、正規に登録されていると判断した場合にステップ S 9 9－2 以降の処理を行う。

また、SAM 3 0 5₂ は、SAM 3 0 5₁ がホームネットワーク内の SAM であるか否かの検証も行う。

【0 3 9 9】

ステップ S 9 9－2：前述したステップ S 9 9－4－2 に対応する処理として、SAM 3 0 5₂ は、SAM 3 0 5₁ との間で相互認証を行って得たセッション鍵データ K_{SES} を共有する。

ステップ S 9 9－3：SAM 3 0 5₂ の SAM 管理部 1 9 0 は、図 9 4 に示すように、ネットワーク機器 3 6 0₁ の SAM 3 0 5₁ からセキュアコンテナ 3 0 4 x を入力する。

ステップ S 9 9－4：暗号化・復号部 1 7 1 は、ステップ S 9 9－2 で共有したセッション鍵データ K_{SES} を用いて、SAM 管理部 1 9 0 を介して入力したセ

キュアコンテナ 304x を復号する。

【0400】

ステップ S99-5: セッション鍵データ K_{SES} を用いて復号されたセキュアコンテナ 304x 内のコンテンツファイル CF が、図 94 に示すメディア・ドラブ SAM260 におけるセクタライズ (Sectorize)、セクタヘッダの付加処理、スクランブル処理、ECC エンコード処理、変調処理および同期処理を経て、RAM 型の記録媒体 130_4 の RAM 領域 134 に記録される。

【0401】

ステップ S99-6: セッション鍵データ K_{SES} を用いて復号されたセキュアコンテナ 304x 内の署名データ $SIG_{6,CP}$, $SIG_{62,SP}$, $SIG_{41,SAM1}$ と、キーファイル KF およびその署名データ $SIG_{7,CP}$, $SIG_{63,SP}$, $SIG_{42,SAM1}$ と、キーファイル KF_1 およびそのハッシュ値 H_{K1} と、公開鍵署名データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ と、公開鍵署名データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とが、作業用メモリ 200 に書き込まれる。

【0402】

ステップ S99-7: 署名処理部 589 において、作業用メモリ 200 から読み出された署名データ $SIG_{61,ESC}$, $SIG_{1,ESC}$, $SIG_{22,ESC}$ が、記憶部 192 から読み出した公開鍵データ $K_{ESC,P}$ を用いて検証され、公開鍵証明書データ CER_{SP} , CER_{CP} , CER_{SAM1} の正当性が確認される。

そして、署名処理部 589 において、公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{6,CP}$ の正当性が検証され、コンテンツファイル CF の作成者の正当性が確認される。署名処理部 589 において、公開鍵証明書データ CER_{SP} に格納された公開鍵データ $K_{SP,P}$ を用いて、署名データ $SIG_{62,CP}$ の正当性が検証され、コンテンツファイル CF の送信者の正当性が確認される。また、署名処理部 189 において、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{SAM1,P}$ を用いて、署名データ $SIG_{41,SAM1}$ の正当性が検証され、コンテンツファイル CF の送信者の正当性が確認される。

【0403】

ステップ S99-8 : 署名処理部 589 において、公開鍵証明書データ CER_{CP} , CER_{SP} , CER_{SAM1} に格納された公開鍵データ $K_{CP,P}$, $K_{SP,P}$, $K_{SAM1,P}$ を用いて、作業用メモリ 200 に記憶されている署名データ $SIG_{7,CP}$, $SIG_{63,SP}$, $SIG_{42,SAM1}$ の正当性を検証する。そして、署名データ $SIG_{7,CP}$, $SIG_{63,SP}$, $SIG_{42,SAM1}$ が正当であると検証されたときに、キーファイル KF の送信者の正当性が確認される。

【0404】

ステップ S99-9 : 署名処理部 589 において、記憶部 192 から読み出した公開鍵データ $K_{ESC,P}$ を用いて、図 97 (B) のキーファイル KF に格納されが署名データ $SIG_{K1,ESC}$ の検証が行われる。そして、署名データ $SIG_{K1,ESC}$ が正当であると検証されたときに、キーファイル KF の作成者の正当性が確認される。

【0405】

ステップ S99-10 : 署名処理部 189 は、ハッシュ値 H_{K1} の正当性を検証し、キーファイル KF_1 の作成者および送信者の正当性を確認する。

なお、当該例では、キーファイル KF_1 の作成者と送信元とが同じ場合を述べたが、キーファイル KF_1 の作成者と送信元とが異なる場合には、キーファイル KF_1 に対して作成者の署名データと送信者と署名データとが作成され、署名処理部 189 において、双方の署名データの正当性が検証される。

【0406】

ステップ S99-11 : 利用監視部 186 は、ステップ S99-10 で復号されたキーファイル KF_1 に格納された利用制御データ 166 を用いて、以後のコンテンツデータ C の購入・利用形態を制御する。

【0407】

ステップ S99-12 : ユーザは、購入・利用形態決定操作部 165 を操作して購入形態を決定し、当該操作に応じた操作信号 $S165$ が、課金処理部 587 に出力される。

ステップ S99-13 : 課金処理部 587 は、操作信号 $S165$ に基づいて、

外部メモリ 2 0 1 に記憶されている利用履歴データ 3 0 8 を更新する。

また、課金処理部 5 8 7 は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ 1 6 6 を更新する。

【0 4 0 8】

ステップ S 9 9－1 4：暗号化・復号部 1 7 3 は、記憶部 1 9 2 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を順に用いて、ステップ S 9 9－1 2 で生成された利用制御データ 1 6 6 を暗号化してメディア・ドライブ SAM 管理部 8 5 5 に出力する。

ステップ S 9 9－1 5：メディア・ドライブ SAM 管理部 8 5 5 は、新たな利用制御データ 1 6 6 を格納したキーファイル KF_1 を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ECC エンコード処理、変調処理および同期処理を経て、RAM 型の記録媒体 130_4 のセキュア RAM 領域 1 3 2 に記録する。

ステップ S 9 9－1 6：キーファイル KF が作業用メモリ 2 0 0 から読み出され、メディア・ドライブ SAM 管理部 8 5 5 を介して、図 9 4 に示すメディア・ドライブ SAM 2 6 0 によって RAM 型の記録媒体 130_4 のセキュア RAM 領域 1 3 2 に書き込まれる。

【0 4 0 9】

ステップ S 9 9－1 7：CPU 1 1 0 0 は、上述した処理が適切に行われたか否かを、外部割り込みでホスト CPU 8 1 0 に通知する。

なお、CPU 1 1 0 0 は、上述した処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU 8 1 0 がポーリングによって当該フラグを読んでもよい。

【0 4 1 0】

なお、SAM 3 0 5₁ における ROM 型の記録媒体のコンテンツデータの購入形態決定処理、ROM 型の記録媒体のコンテンツデータの購入形態を決定した後に RAM 型の記録媒体に書き込む場合の処理は、サービスプロバイダ 3 1 0 において秘密鍵データ $K_{SP,P}$ を用いて付けられた署名データ SIG_{SP} の検証処理を行う点を除いて、前述した第 1 実施形態の SAM 1 0 5₁ における処理と同じであ

る。

また、SAM305₁の実現方法も、前述した第1実施形態で説明したSAM105₁の実現方法と同じである。

また、ユーザホームネットワーク303に用いられる機器においても、第1実施形態で説明した図63に示す構成は同様に適用される。また、この場合に、SAM305₁、AV圧縮・伸長用SAM163、メディア・ドラブSAM260およびメディアSAM133の回路モジュールとして、図64～図79を用いて説明した構成が同様に適用される。

また、図62を用いて説明したセキュア機能も、コンテンツプロバイダ101がサービスプロバイダ310に置き換える点を除いて、EMDシステム300でも同様に適用される。

【0411】

以下、ユーザホームネットワーク303における各種の機器の接続形態等を再び説明する。

図101は、ユーザホームネットワーク303における機器の接続形態の一例を説明するための図である。

ここでは、図101に示すように、ユーザホームネットワーク303内でネットワーク機器360₁、AV機器360₂、360₃がIEEE1394シリアルバス191を介して接続されている場合を説明する。

ネットワーク機器360₁は、外部メモリ201、SAM305₁、CAモジュール311、AV圧縮・伸長用SAM163およびダウンロードメモリ167を有する。

CAモジュール311は、公衆回線などのネットワークを介して、サービスプロバイダ310と通信を行う。

また、SAM305₁は、公衆回線などのネットワークを介して、EMDサービスセンタ302と通信を行う。

ダウンロードメモリ167としては、メディアSAM167aを備えたメモリスティック、あるいはHDDなどが用いられる。ダウンロードメモリ167には、サービスプロバイダ310からダウンロードしたセキュアコンテナ304など

が記憶される。

各機器には、A T R A C 3やM P E Gなどの各種の圧縮・伸長方式にそれぞれ対応した複数のA V圧縮・伸長用S A M 1 6 3が内蔵されている。

S A M 3 0 5₁ は、接触方式あるいは非接触方式のI Cカード1 1 4 1と通信を行うことが可能である。I Cカード1 1 4 1は、ユーザI Dなどの各種のデータが記憶しており、S A M 3 0 5₁ においてユーザ認証を行う場合などに用いられる。

【0 4 1 2】

A V機器3 6 0₂ は、例えば、ストレージ機器であり、S A M 3 0 5₁ と3 0 5₂ との間で所定の処理を経て、I E E E 1 3 9 4シリアルバス1 9 1を介してネットワーク機器3 6 0₁ から入力したセキュアコンテナを記録媒体1 3 0に記録する。

また、A V機器3 6 0₃ も同様に、例えば、ストレージ機器であり、S A M 3 0 5₂ と3 0 5₃ との間で所定の処理を経て、I E E E 1 3 9 4シリアルバス1 9 1を介してA V機器3 6 0₂ から入力したセキュアコンテナを記録媒体1 3 0に記録する。

【0 4 1 3】

なお、図1 0 1に示す例では、記録媒体1 3 0にメディアS A M 1 3 3が搭載されている場合を例示したが、例えば、記録媒体1 3 0のメディアS A M 1 3 3が搭載されていない場合には、図1 0 1に点線で示したように、メディア・ドラブS A M 2 6 0を用いて、S A M 3 0 5₂ , 3 0 5₃ との間の認証が行われる。

【0 4 1 4】

次に、図8 2に示すE M Dシステム3 0 0の全体動作について説明する。

図1 0 2および図1 0 3は、E M Dシステム3 0 0の全体動作のフローチャートである。

ここでは、サービスプロバイダ3 1 0からユーザホームネットワーク3 0 3にオンラインでセキュアコンテナ3 0 4を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、E M Dサービスセンタ3 0 2へのコンテンツプロバイダ3 0 1、サービスプロバイダ3 1 0およびS A M 3 0 5₁ ~3 0

5₄ の登録は既に終了しているものとする。

【0 4 1 5】

ステップ S 2 1 : EMD サービスセンタ 3 0 2 は、コンテンツプロバイダ 3 0 1 の公開鍵データ $K_{CP,P}$ の公開鍵証明書 CER_{CP} を、自らの署名データ $SIG_{1,ESC}$ と共にコンテンツプロバイダ 3 0 1 に送信する。

また、EMD サービスセンタ 3 0 2 は、コンテンツプロバイダ 3 0 1 の公開鍵データ $K_{SP,P}$ の公開鍵証明書 CER_{SP} を、自らの署名データ $SIG_{61,ESC}$ と共にサービスプロバイダ 3 1 0 に送信する。

また、EMD サービスセンタ 3 0 2 は、各々有効期限が 1 カ月の 3 カ月分のライセンス鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク 3 0 3 の $SAM_{305_1 \sim 305_4}$ に送信する。

【0 4 1 6】

ステップ S 2 2 : コンテンツプロバイダ 3 0 1 は、相互認証を行った後に、権利書データ 1 0 6 およびコンテンツ鍵データ K_c を EMD サービスセンタ 3 0 2 に登録して権威化する。

また、EMD サービスセンタ 3 0 2 は、図 3 (B) に示す 6 カ月分のキーファイル KF を作成し、これをコンテンツプロバイダ 3 0 1 に送信する。

【0 4 1 7】

ステップ S 2 3 : コンテンツプロバイダ 3 0 1 は、図 3 (A), (B) に示すコンテンツファイル CF およびその署名データ $SIG_{6,CP}$ と、キーファイル KF およびその署名データ $SIG_{7,CP}$ とを作成し、これらと図 3 (C) に示す公開鍵証明書データ CER_{cp} およびその署名データ $SIG_{1,ESC}$ とを格納したセキュアコンテナ 1 0 4 を、オンラインおよび／またはオフラインで、サービスプロバイダ 3 1 0 に提供する。

【0 4 1 8】

ステップ S 2 4 : サービスプロバイダ 3 1 0 は、図 3 (C) に示す署名データ $SIG_{1,ESC}$ を検証した後に、公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP,P}$ を用いて、図 3 (A), (B) に示す署名データ $SIG_{6,CP}$ および $SIG_{7,CP}$ を検証して、セキュアコンテナ 1 0 4 が正当なコンテンツプロバイダ

301から送信されたものであるかを確認する。

【0419】

ステップS25：サービスプロバイダ310は、プライスタグデータ312およびその署名データ $SIG_{64,SP}$ を作成し、これらを格納した図87に示すセキュアコンテナ304を作成する。

【0420】

ステップS26：サービスプロバイダ310は、プライスタグデータ312をEMDサービスセンタ302に登録して権威化する。

【0421】

ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図89に示すネットワーク機器360₁の復号モジュール905に送信する。

【0422】

ステップS28：CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0423】

ステップS29：SAM305₁～305₄のいずれかにおいて、図84（D）に示す署名データ $SIG_{61,ESC}$ を検証した後に、公開鍵証明書データ CER_{SP} に格納された公開鍵データ $K_{SP,P}$ を用いて、図84（A），（B），（C）に示す署名データ $SIG_{62,SP}$ ， $SIG_{63,SP}$ ， $SIG_{64,SP}$ を検証して、セキュアコンテナ304内の所定のデータが正当なサービスプロバイダ310において作成および送信されたか否かを確認する。

【0424】

ステップS30：SAM305₁～305₄のいずれかにおいて、図84（D）に示す署名データ $SIG_{1,ESC}$ を検証した後に、公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP,P}$ を用いて、図84（A），（B），（C）に示す署名データ $SIG_{6,SP}$ ， $SIG_{7,SP}$ を検証して、セキュアコンテナ304内のコンテンツファイルCFが正当なコンテンツプロバイダ301において作成され

たか否かと、キーファイル K F が正当なコンテンツプロバイダ 3 0 1 から送信されたか否かを確認する。

また、SAM 3 0 5₁ ～ 3 0 5₄ のいずれかにおいて、公開鍵データ K_{ESC,P} を用いて、図 8 4 (B) に示すキーファイル K F 内の署名データ S I G_{K1,ESC} の正当性を検証することで、キーファイル K F が正当な EMD サービスセンタ 3 0 2 によって作成されたか否かを確認する。

【0 4 2 5】

ステップ S 3 1 : ユーザが図 8 8 に示す操作部 1 6 5 を操作してコンテンツの購入・利用形態を決定する。

【0 4 2 6】

ステップ S 3 2 : ステップ S 3 1 においてホスト CPU 8 1 0 から SAM 3 0 5₁ ～ 3 0 5₄ に出された内部割り込み S 8 1 0 に基づいて、SAM 3 0 5₁ ～ 3 0 5₄ において、セキュアコンテナ 3 0 4 の利用履歴 (Usage Log) データ 3 0 8 が生成される。

SAM 3 0 5₁ ～ 3 0 5₄ から EMD サービスセンタ 3 0 2 に、利用履歴データ 3 0 8 およびその署名データ S I G_{205,SAM1} が送信される。

また、購入形態が決定される度にリアルタイムに、SAM 3 0 5₁ ～ 3 0 5₄ から EMD サービスセンタ 3 0 2 に利用制御状態データ 1 6 6 が送信される。

【0 4 2 7】

ステップ S 3 3 : EMD サービスセンタ 3 0 2 は、利用履歴データ 3 0 8 に基づいて、コンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 の各々について、課金内容を決定 (計算) し、その結果に基づいて、決済請求権データ 1 5 2 c, 1 5 2 s を作成する。

【0 4 2 8】

ステップ S 3 4 : EMD サービスセンタ 3 0 2 は、ペイメントゲートウェイ 9 0 を介して決済機関 9 1 に、決済請求権データ 1 5 2 c, 1 5 2 s を自らの署名データと共に送信し、これにより、ユーザホームネットワーク 3 0 3 のユーザが決済機関 9 1 に支払った金銭が、コンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 の所有者に分配される。

【0429】

以上説明したように、EMDシステム300では、図3に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305₁～305₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₃を用いて暗号化されており、配信鍵データKD₁～KD₃を保持しているSAM305₁～305₄内でのみ復号される。そして、SAM305₁～305₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

【0430】

従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ301の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300によれば、権利書データ106をサービスプロバイダ310が管理できないようできる。

そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303のSAMにおける当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

【0431】

また、EMDシステム300では、セキュアコンテナ104、304内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ310およびSAM305

$1 \sim 305_4$ において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータ C の不正利用を効果的に回避できる。

【0432】

また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク303へのコンテンツデータ C の配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM305 $_1 \sim 305_4$ におけるコンテンツデータ C の権利処理を共通化できる。

【0433】

また、EMDシステム300では、ユーザホームネットワーク303内のネットワーク機器360 $_1$ およびAV機器360 $_2 \sim 360_4$ においてコンテンツデータ C を購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

例えば、図104に示すように、コンテンツプロバイダ301が提供したコンテンツデータ C を、サービスプロバイダ310からユーザホームネットワーク303に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク303、303aのSAMにおいて、コンテンツプロバイダ301が作成した権利書データ106に基づいて、共通の権利処理ルールが採用される。

【0434】

また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービス

プロバイダ 310 のサービス形態とは無関係に、そのまま SAM305₁ ~ 305₄ に供給される。従って、SAM305₁ ~ 305₄ において、権利書データ 106 に基づいて、コンテンツプロバイダ 301 の意向通りに、コンテンツファイル CF の利用を行わせることができる。

すなわち、EMD システム 300 によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織 725 に頼ることなく、技術的な手段によって、コンテンツプロバイダ 301 の所有者の権利および利益を確実に守ることができる。

【0435】

以下、上述した第 2 実施形態の EMD システム 300 で採用するセキュアコンテナなどの配送プロトコルについて説明する。

図 105 に示すように、コンテンツプロバイダ 301 において作成されたセキュアコンテナ 104 は、インターネット (TCP/IP) あるいは専用線 (ATM Cell) などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバイダ 310 に提供される。

また、サービスプロバイダ 310 は、セキュアコンテナ 104 を用いて作成したセキュアコンテナ 304 を、デジタル放送 (MPEG-TS 上の XML/SMIL)、インターネット (TCP/IP 上の XML/SMIL) あるいはパッケージ流通 (記録媒体) などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク 303 に配給する。

また、ユーザホームネットワーク 303、303a 内、あるいはユーザホームネットワーク 303 と 303a との間において、SMA 相互間で、セキュアコンテナが、家庭内 EC (Electric Commerce) / 配信サービス (1394 シリアルバス・インターフェイス上の XML/SMIL) や記録媒体などを用いて転送される。

【0436】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、EMD サービスセンタ 102、302 において、キーファイル KF を作成する場合を例示したが、コンテンツプロバイダ 10

1, 3 0 1においてキーファイルK Fを作成してもよい。

【0 4 3 7】

【発明の効果】

以上説明したように、本発明のデータ処理装置によれば、コンテンツデータの取り扱いを示す権利書データに基づいたコンテンツデータの権利処理をセキュアな環境で行うことができる。

その結果、権利書データをコンテンツデータの提供に係わる者が作成すれば、コンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の第 1 実施形態の EMD システムの全体構成図である。

【図 2】

図 2 は、本発明のセキュアコンテナの概念を説明するための図である。

【図 3】

図 3 は、図 1 に示すコンテンツプロバイダから S A M に送信されるセキュアコンテナのフォーマットを説明するための図である。

【図 4】

図 4 は、図 3 に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図 5】

図 5 は、図 3 に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図 6】

図 6 は、図 1 に示すコンテンツプロバイダと EMD サービスセンタとの間で行われる登録およびキーファイルの転送を説明するための図である。

【図 7】

図 7 は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図 8】

図 8 は、コンテンツ ID を説明するための図である。

【図 9】

図 9 は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図 1 0】

図 1 0 は、セキュアコンテナのハイパーリンク構造を説明するための図である。

【図 1 1】

図 1 1 は、本実施形態で用いられる ROM 型の記録媒体の第 1 の例を説明するための図である。

【図 1 2】

図 1 2 は、本実施形態で用いられる ROM 型の記録媒体の第 2 の例を説明するための図である。

【図 1 3】

図 1 3 は、本実施形態で用いられる ROM 型の記録媒体の第 3 の例を説明するための図である。

【図 1 4】

図 1 4 は、本実施形態で用いられる RAM 型の記録媒体の第 1 の例を説明するための図である。

【図 1 5】

図 1 5 は、本実施形態で用いられる RAM 型の記録媒体の第 2 の例を説明するための図である。

【図 1 6】

図 1 6 は、本実施形態で用いられる RAM 型の記録媒体の第 3 の例を説明するための図である。

【図 1 7】

図 1 7 は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図 1 8】

図 1 8 は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図 1 9】

図 1 9 は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図 2 0】

図 2 0 は、図 1 に示す EMD サービスセンタの機能を示す図である。

【図 2 1】

図 2 1 は、図 1 に示す利用履歴データを説明するための図である。

【図 2 2】

図 2 2 は、図 1 に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図 2 3】

図 2 3 は、図 2 2 に示すホスト CPU と SAM との関係を説明するための図である。

【図 2 4】

図 2 4 は、SAM を実現するソフトウェア構成を説明するための図である。

【図 2 5】

図 2 5 は、ホスト CPU に出される外部割り込みを説明するための図である。

【図 2 6】

図 2 6 は、ホスト CPU が出す内部割り込みを説明するための図である。

【図 2 7】

図 2 7 は、ホスト CPU が出すファンクションコールを説明するための図である。

【図 2 8】

図 2 8 は、SAM の C P O U の処理状態を説明するための図である。

【図 2 9】

図 2 9 は、ホスト CPU および SAM のメモリ空間を説明するための図である。

【図 3 0】

図 3 0 は、図 1 に示すユーザホームネットワーク内の S A M の機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図 3 1】

図 3 1 は、図 2 2 に示す外部メモリに記憶されるデータを説明するための図である。

【図 3 2】

図 3 2 は、作業用メモリに記憶されるデータを説明するための図である。

【図 3 3】

図 3 3 は、図 1 に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図 3 4】

図 3 4 は、図 3 0 に示す記憶部に記憶されるデータを説明するための図である。

【図 3 5】

図 3 5 は、EMD サービスセンタからライセンス鍵データを受信する際の S A M の処理を示すフローチャートである。

【図 3 6】

図 3 6 は、セキュアコンテナを入力する際の S A M の処理を示すフローチャートである。

【図 3 7】

図 3 7 は、図 1 に示すユーザホームネットワーク内の S A M の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図 3 8】

図 3 8 は、コンテンツデータの購入形態を決定する際の S A M の処理を示すフローチャートである。

【図 3 9】

図 3 9 は、購入形態が決定されたセキュアコンテナを説明するための図である。

【図 4 0】

図 4 0 は、コンテンツデータを再生する際の S A M の処理を示すフローチャートである。

【図 4 1】

図 4 1 は、図 2 2 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送し、A V 機器において再購入を行う場合を説明するための図である。

【図 4 2】

図 4 2 は、図 4 1 に示す場合における転送元の S A M 内でのデータの流れを示す図である。

【図 4 3】

図 4 3 は、図 4 2 に示す場合の処理を示すフローチャートである。

【図 4 4】

図 4 4 は、図 4 1 において転送されるセキュアコンテナのフォーマットを説明するための図である。

【図 4 5】

図 4 5 は、図 4 1 に示す場合において、転送先の S A M において、入力したコンテンツファイルなどを、R A M 型あるいは R O M 型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図 4 6】

図 4 6 は、図 4 1 に示す場合における転送先の S A M の処理を示すフローチャートである。

【図 4 7】

図 4 7 は、図 4 1 に示す場合における転送先の S A M の処理を示すフローチャートである。

【図 4 8】

図 4 8 は、図 1 に示すユーザホームネットワーク内の S A M における各種の購入形態を説明するための図である。

【図 4 9】

図 4 9 は、コンテンツの購入形態が未決定の図 1 1 に示す R O M 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、A V 機器において購入形態を決定する場合を説明するための図である。

【図 5 0】

図 5 0 は、図 4 9 に示す場合における A V 機器の S A M 内でのデータの流れを示す図である。

【図 5 1】

図 5 1 は、図 4 9 に示す場合における S A M の処理のフローチャートである。

【図 5 2】

図 5 2 は、ユーザホームネットワーク内の A V 機器において購入形態が未決定の R O M 型の記録媒体からセキュアコンテナを読み出して、これを他の A V 機器に転送して R A M 型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図 5 3】

図 5 3 は、図 5 2 に示す場合における転送元の S A M 内でのデータの流れを示す図である。

【図 5 4】

図 5 4 は、図 5 2 において、転送元の S A M から転送先の S A M に転送されるセキュアコンテナのフォーマットを説明するための図である。

【図 5 5】

図 5 5 は、図 5 2 の場合における、転送元および転送先の S A M の処理のフローチャートを示す図である。

【図 5 6】

図 5 6 は、図 5 2 の場合における、転送元および転送先の S A M の処理のフローチャートを示す図である。

【図 5 7】

図 5 7 は、図 5 2 に示す場合における転送先の S A M 内でのデータの流れを示す図である。

【図 5 8】

図 5 8 は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図 5 9】

図 5 9 は、S A M が作成する S A M 登録リストのデータフォーマットを説明するための図である。

【図 6 0】

図 6 0 は、E M D サービスセンタが作成する公開鍵証明書破棄リストのフォーマットを説明するための図である。

【図 6 1】

図 6 1 は、E M D サービスセンタが作成する S A M 登録リストのデータフォーマットを説明するための図である。

【図 6 2】

図 6 2 は、S A M が持つセキュリティ機能を説明するための図である。

【図 6 3】

図 6 2 は、図 1 に示すユーザホームネットワーク内の例えばネットワーク機器内での各種の S A M に搭載形態の一例を説明するための図である。

【図 6 4】

図 6 4 は、図 6 3 に示すダウンロードメモリ周辺の詳細な回路構成を説明するための図である。

【図 6 5】

図 6 5 は、図 6 3 におけるホスト C P U と S A M との関係を説明するための図である。

【図 6 6】

図 6 6 は、図 6 3 におけるホスト C P U、S A M、A V 圧縮・伸長用 S A M および記録媒体の関係を説明するための図である。

【図 6 7】

図 6 7 は、図 6 3 におけるホスト CPU O、メディア・ドラブ SAM および A V 圧縮・伸長用 SAM の関係を説明するための図である。

【図 6 8】

図 6 8 は、権利処理用の SAM の回路モジュールの第 1 形態を説明するための図である。

【図 6 9】

図 6 9 は、図 6 8 に示す回路モジュールを用いた場合の SAM 内のハードウェア構成の一例を説明するための図である。

【図 7 0】

図 7 0 は、権利処理用の SAM のアドレス空間を説明するための図である。

【図 7 1】

図 7 1 は、ホスト CPU のアドレス空間を説明するための図である。

【図 7 2】

図 7 2 は、権利処理用の SAM の回路モジュールの第 2 形態を説明するための図である。

【図 7 3】

図 7 3 は、メディア SAM の回路モジュールを説明するための図である。

【図 7 4】

図 7 4 は、ROM 型の記録媒体のメディア SAM の出荷時における記憶データを説明するための図である。

【図 7 5】

図 7 5 は、ROM 型の記録媒体のメディア SAM の登録後における記憶データを説明するための図である。

【図 7 6】

図 7 6 は、RAM 型の記録媒体のメディア SAM の出荷時における記憶データを説明するための図である。

【図 7 7】

図 7 7 は、RAM 型の記録媒体のメディア SAM の登録後における記憶データ

を説明するための図である。

【図 78】

図 78 は、AV 圧縮・伸長用 SAM の回路モジュールの第 1 形態を説明するための図である。

【図 79】

図 79 は、メディア・ドライブ SAM の回路モジュールを説明するための図である。

【図 80】

図 80 は、図 1 に示す EMD システムの全体動作のフローチャートである。

【図 81】

図 81 は、第 1 実施形態の EMD システムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図 82】

図 82 は、本発明の第 2 実施形態の EMD システムの全体構成図である。

【図 83】

図 83 は、サービスプロバイダにおいて行われるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図 84】

図 84 は、図 82 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図 85】

図 85 は、図 84 に示すセキュアコンテナに格納されたコンテンツファイルの送信形態を説明するための図である。

【図 86】

図 86 は、図 87 に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図である。

【図 87】

図 87 は、図 81 に示す EMD サービスセンタの機能を示す図である。

【図 8 8】

図 8 8 は、図 8 2 に示すネットワーク機器の構成図である。

【図 8 9】

図 8 9 は、図 8 8 に示す C A モジュールの機能ブロック図である。

【図 9 0】

図 9 0 は、図 8 2 に示す S A M の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図 9 1】

図 9 1 は、図 9 0 に示す作業用メモリに記憶されるデータを説明するための図である。

【図 9 2】

図 9 2 は、図 8 2 に示す S A M の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図 9 3】

図 9 3 は、図 8 2 に示す S A M におけるセキュアコンテナの入力処理の手順を示すフローチャートである。

【図 9 4】

図 9 4 は、図 8 2 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送する場合を説明するための図である。

【図 9 5】

図 9 5 は、図 8 2 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送する場合の転送元の S A M 内での処理の流れを説明するための図である。

【図 9 6】

図 9 6 は、図 9 5 に示す転送元の S A M の処理を示すフローチャートである。

【図 9 7】

図 9 7 は、図 9 4 に示す場合に、転送元の S A M から転送先の S A M に転送されるセキュアコンテナのフォーマットを示す図である。

【図 9 8】

図 9 8 は、図 9 4 に示す場合の転送先の S A M 内でのデータの流れを示す図である。

【図 9 9】

図 9 9 は、図 9 4 に示す場合の転送先の S A M の処理のフローチャートである。

【図 1 0 0】

図 1 0 0 は、図 9 4 に示す場合の転送先の S A M の処理のフローチャートである。

【図 1 0 1】

図 1 0 1 は、図 8 2 に示すユーザホームネットワーク内での S A M の接続形態の一例を説明するための図である。

【図 1 0 2】

図 1 0 2 は、図 8 2 に示す E M D システムの全体動作のフローチャートである。

【図 1 0 3】

図 1 0 3 は、図 8 2 に示す E M D システムの全体動作のフローチャートである。

【図 1 0 4】

図 1 0 4 は、図 8 2 に示す E M D システムのサービス形態の一例を示す図である。

【図 1 0 5】

図 1 0 5 は、図 8 2 に示す E M D システムにおいて採用されるセキュアコンテンツの配送プロトコルを説明するための図である。

【図 1 0 6】

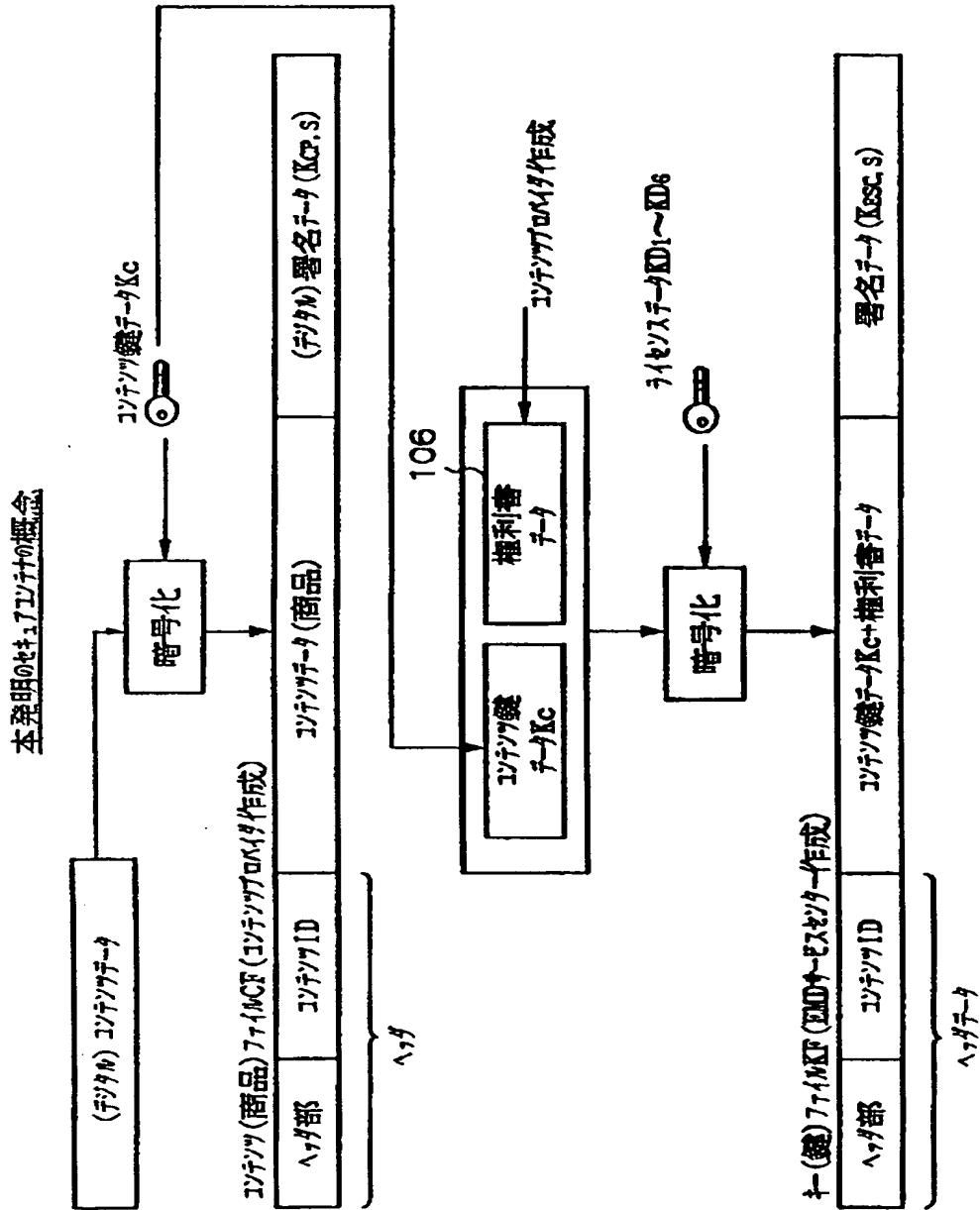
図 1 0 6 は、従来の E M D システムの構成図である。

【符号の説明】

9 0 … ペイメントゲートウェイ、9 1 … 決済機関、9 2 … ルート認証局、1 0 0, 3 0 0 … E M D システム、1 0 1, 3 0 1 … コンテンツプロバイダ、1 0 2

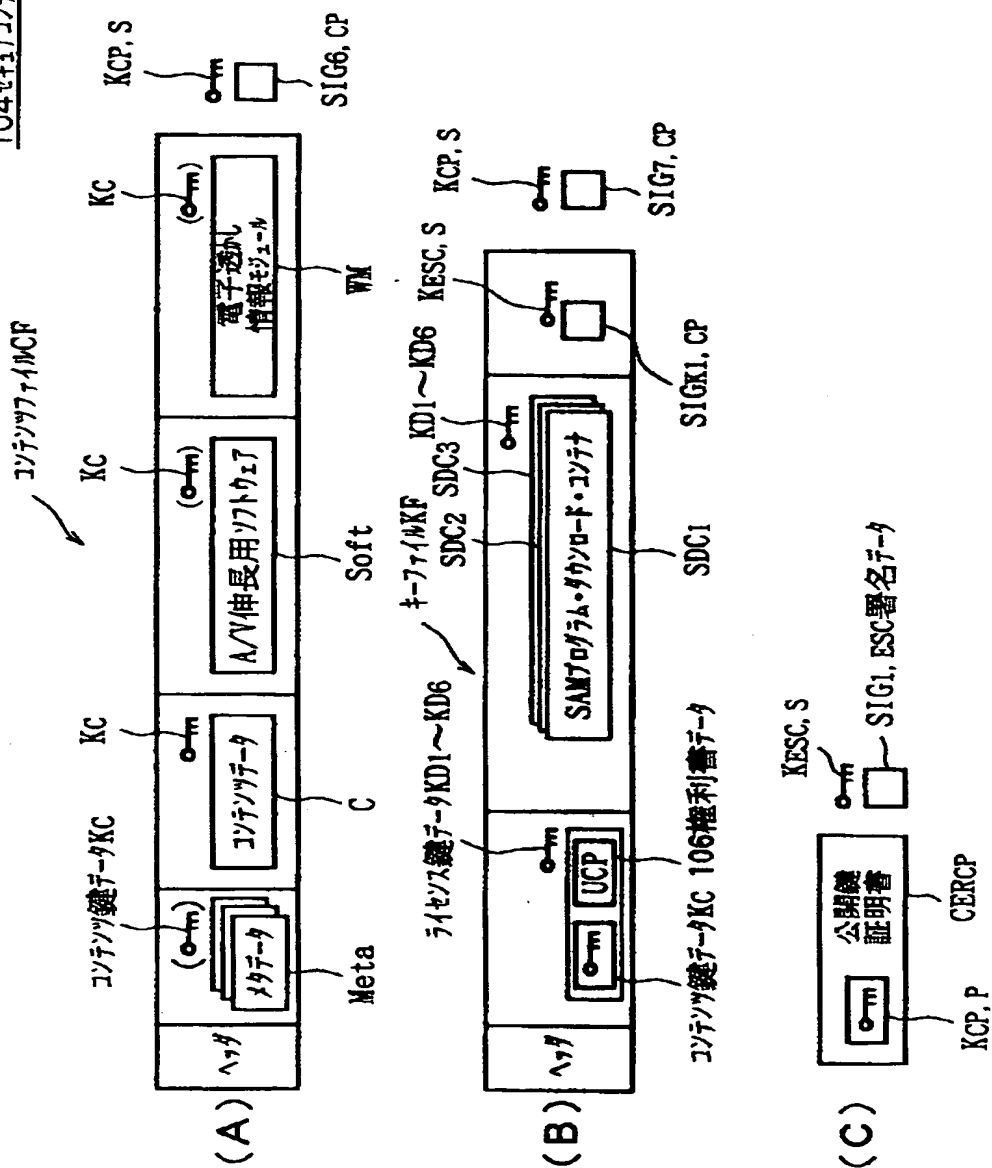
、302…EMDサービスセンタ、103、303…ユーザホームネットワーク、104、304…セキュアコンテナ、105₁～105₄、305₁～305₄…SAM、106…権利書データ、107、307…決済レポートデータ、108、308…利用履歴データ、160₁…ネットワーク機器、160₂～160₄…AV機器、152、152c、152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

【图 2】

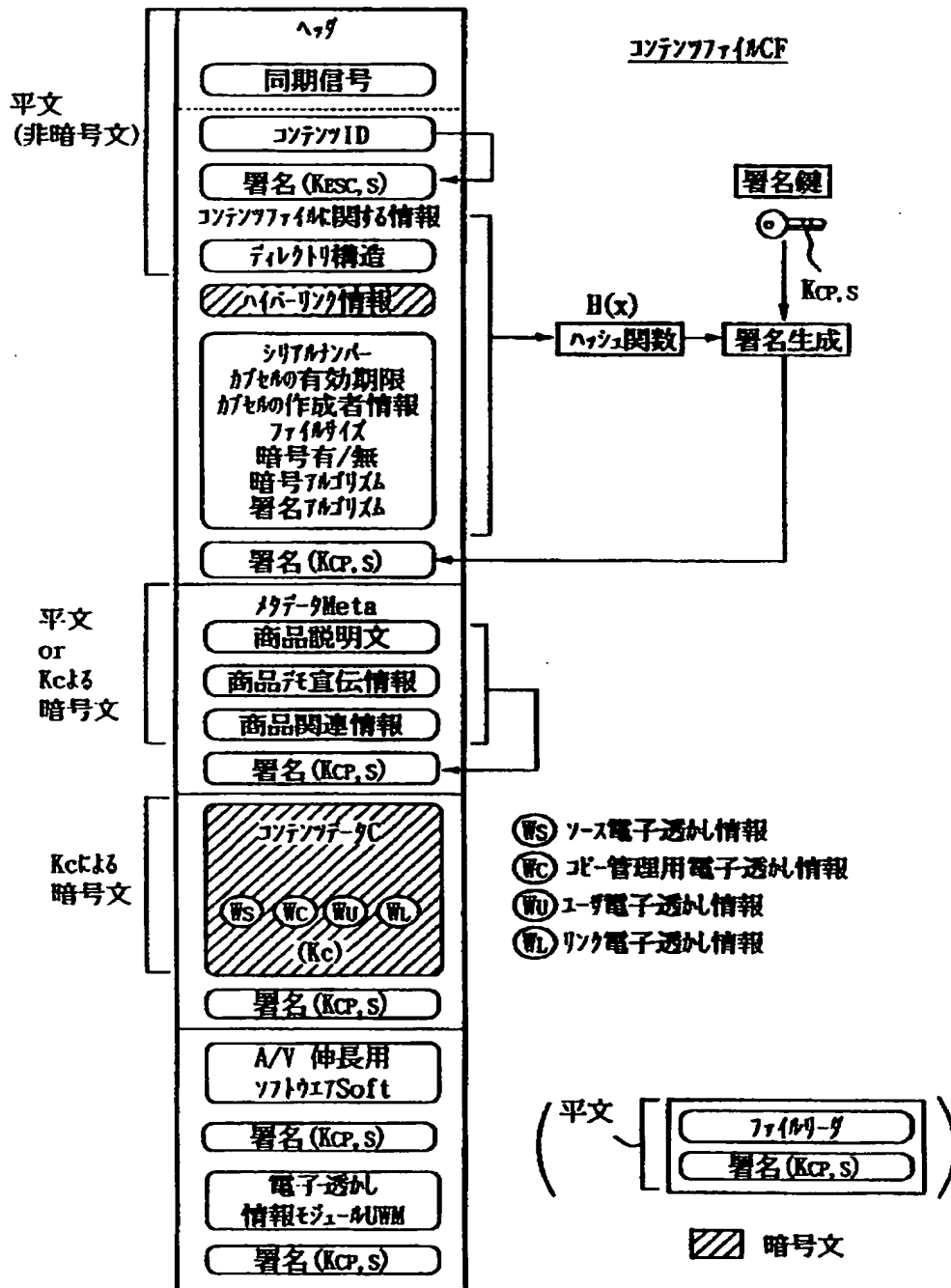


【図 3】

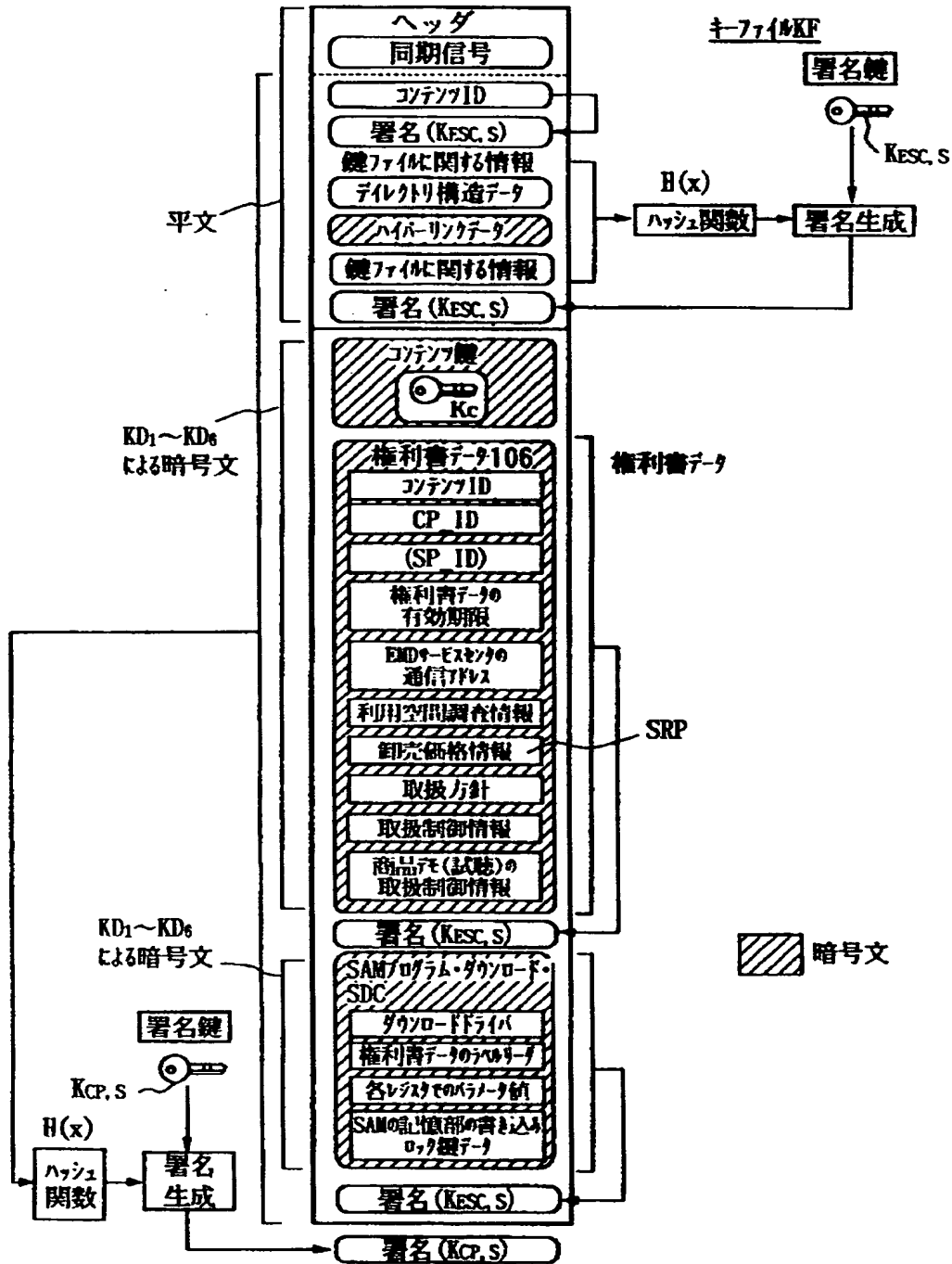
104 セキュリティコンテナ



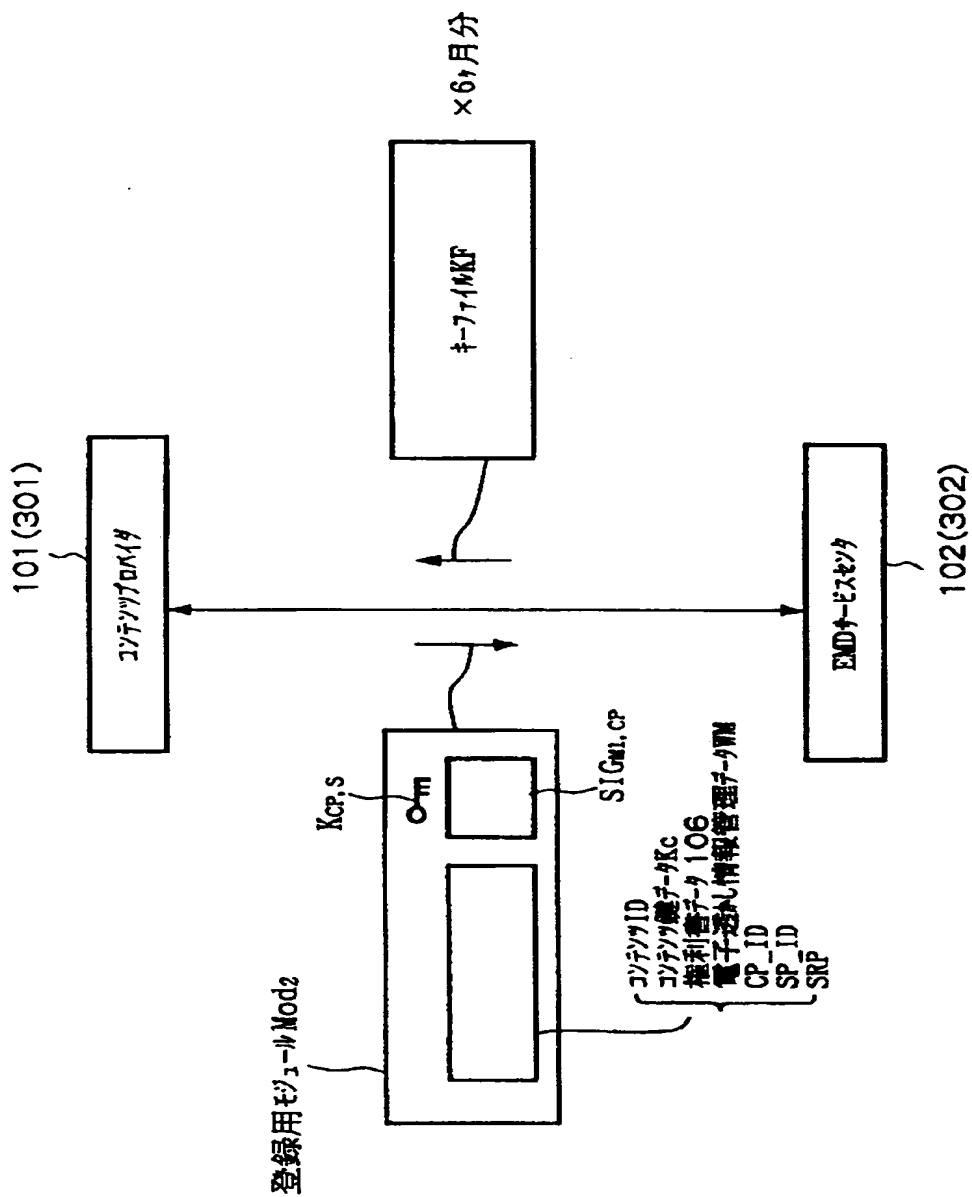
【図 4】



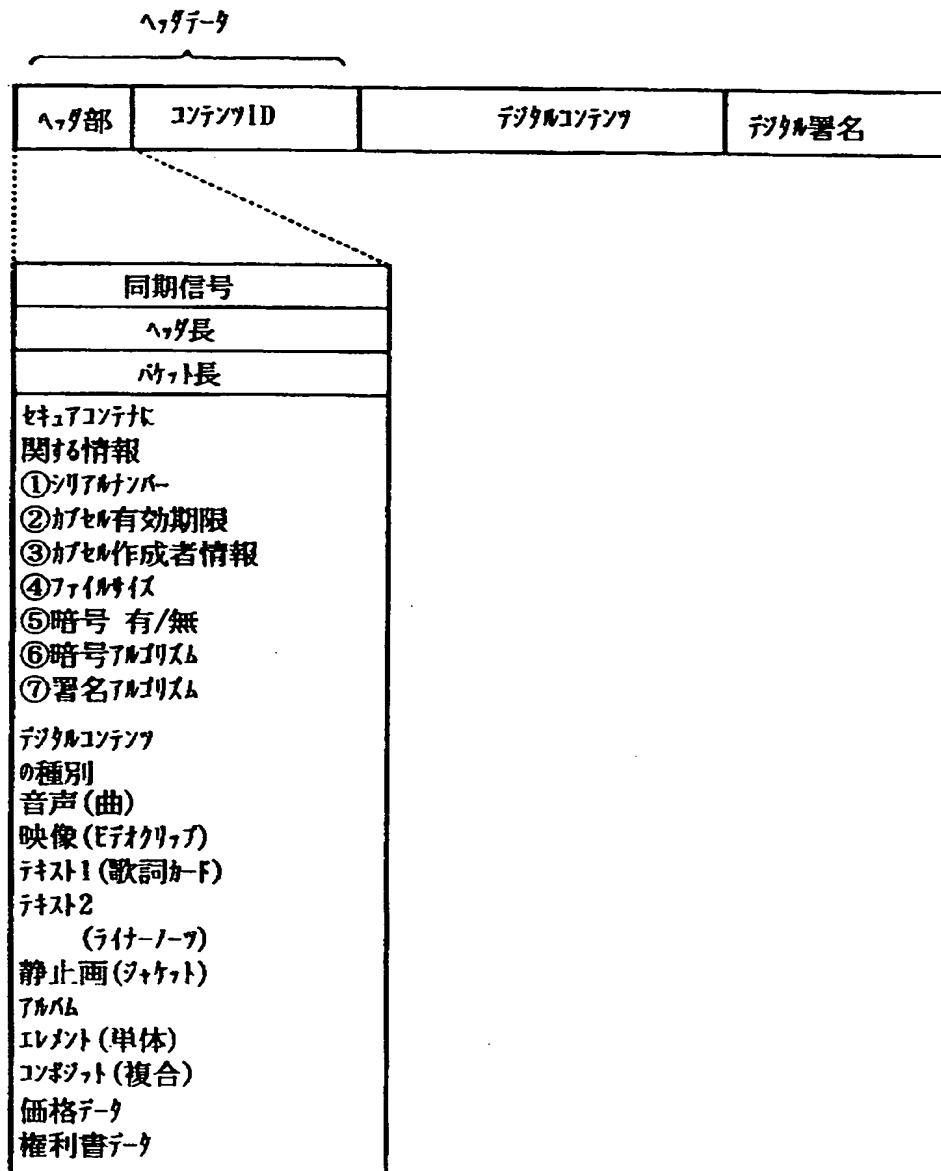
【図 5】



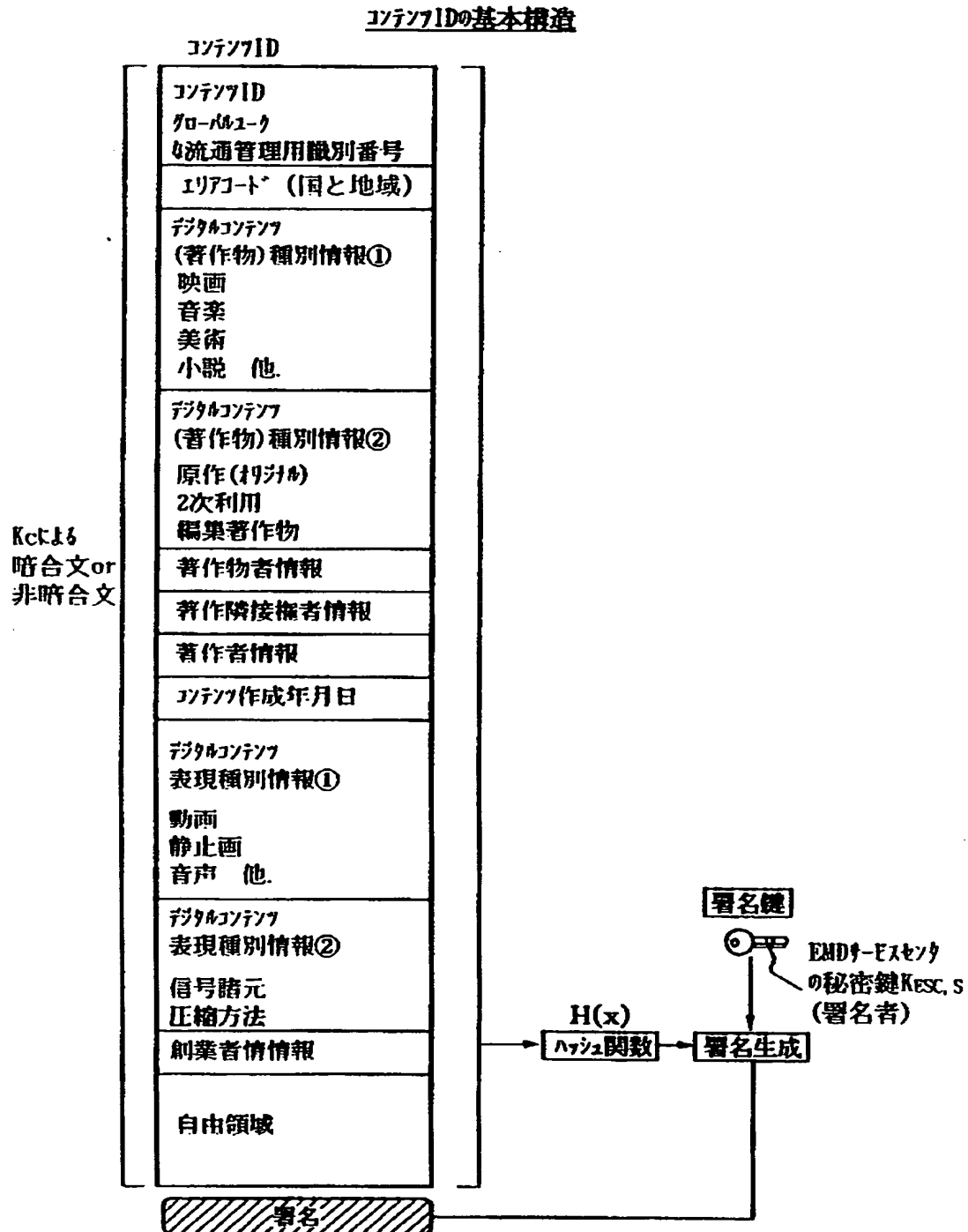
【図 6】



【図 7】

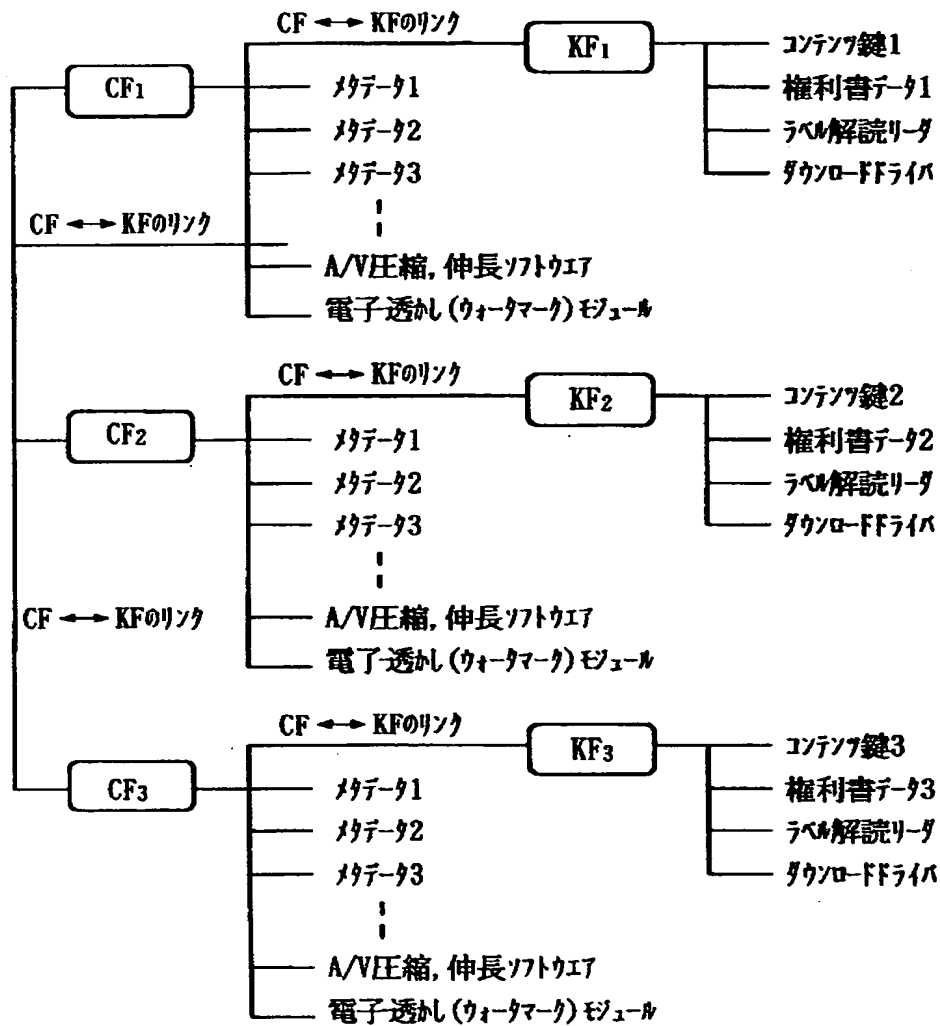


【図 8】

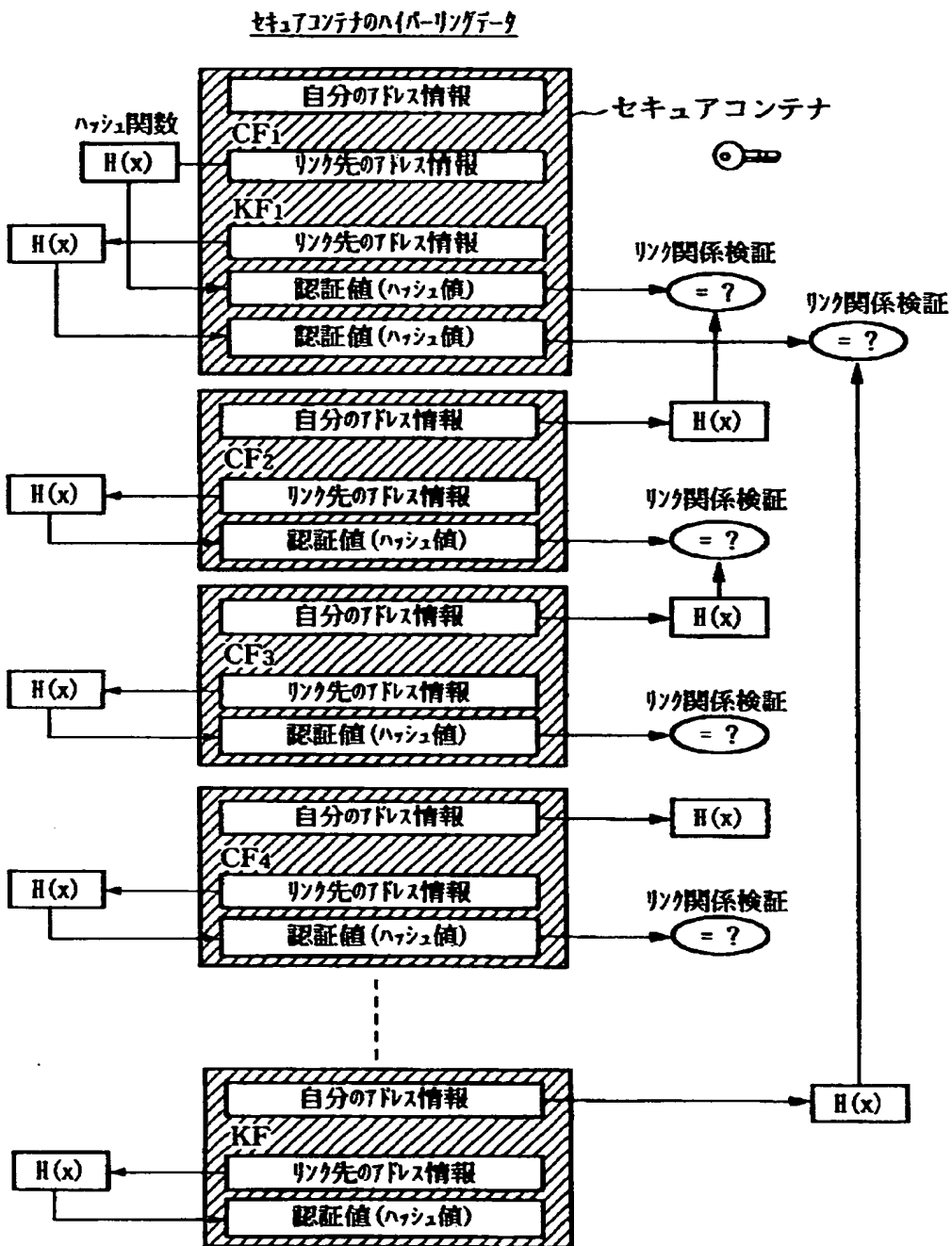


【図 9】

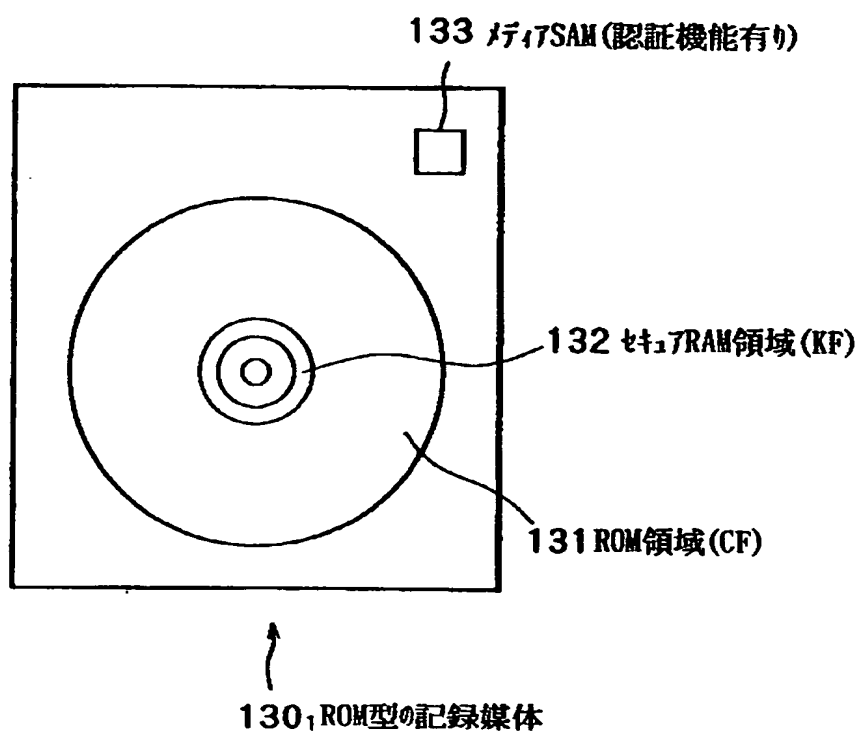
セキュアコンテンツのディレクトリ構造



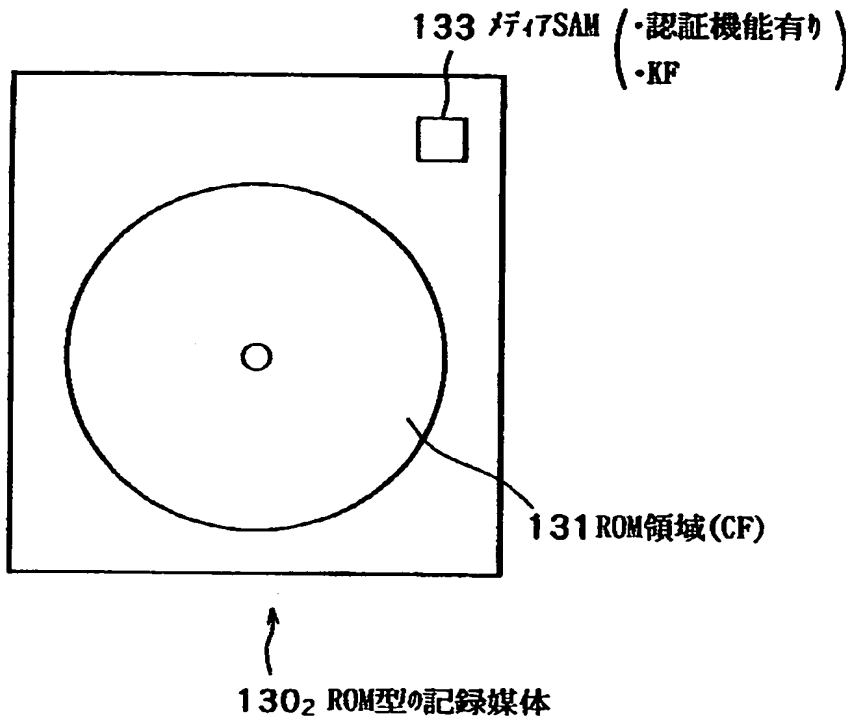
【図 1 0】



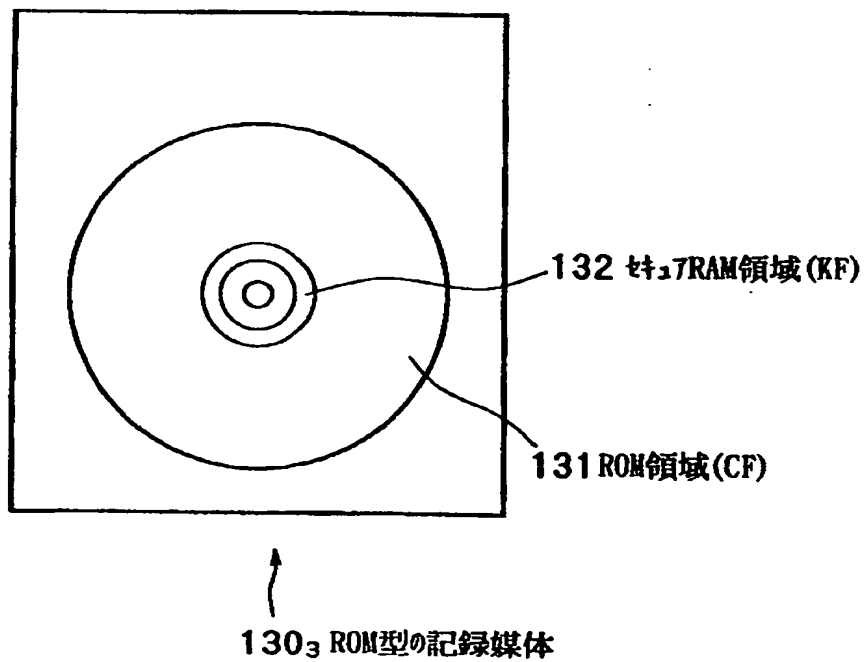
【図 1 1】



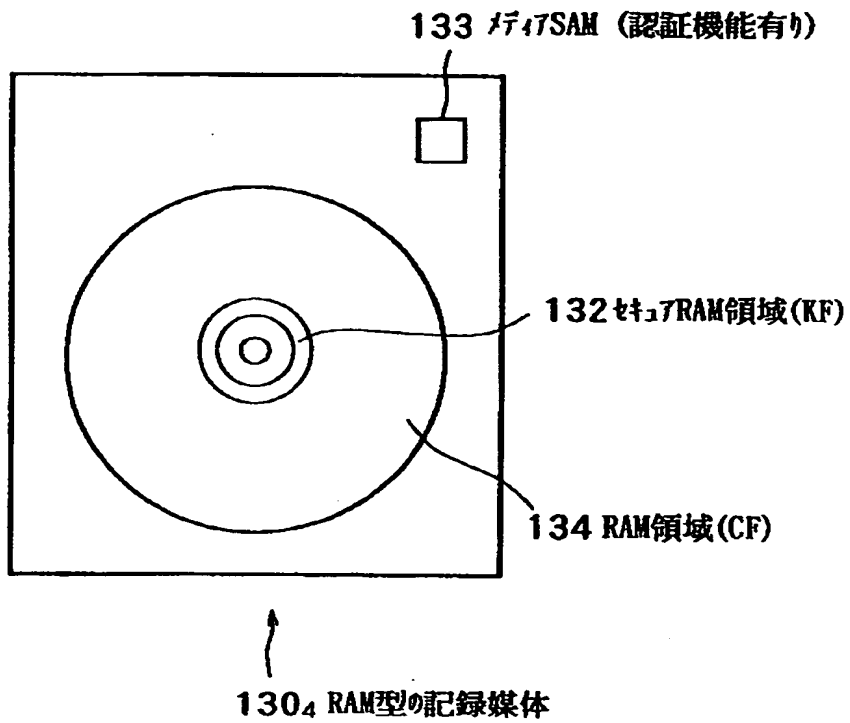
【図 1 2】



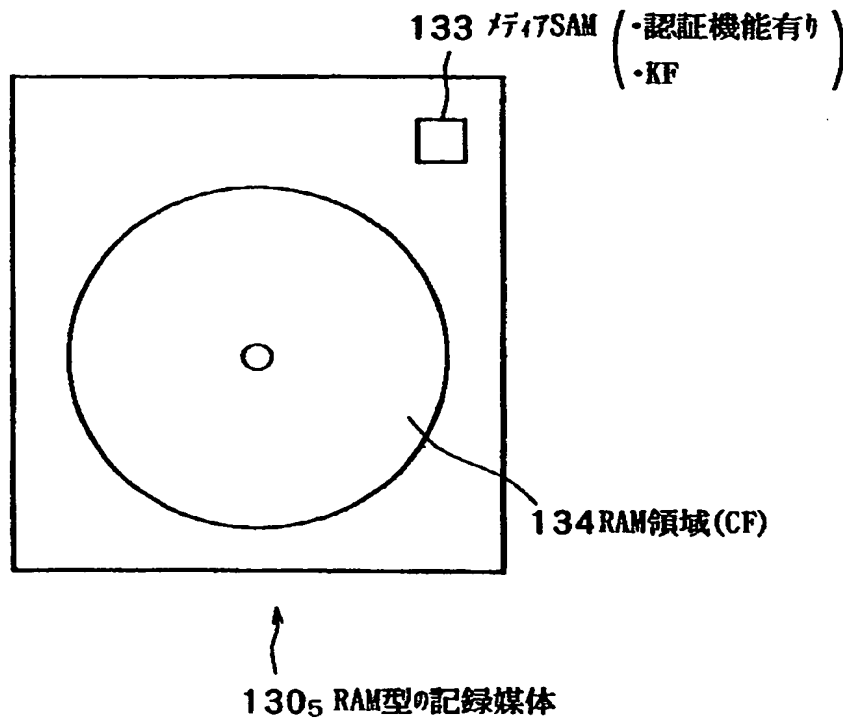
【図 1 3】



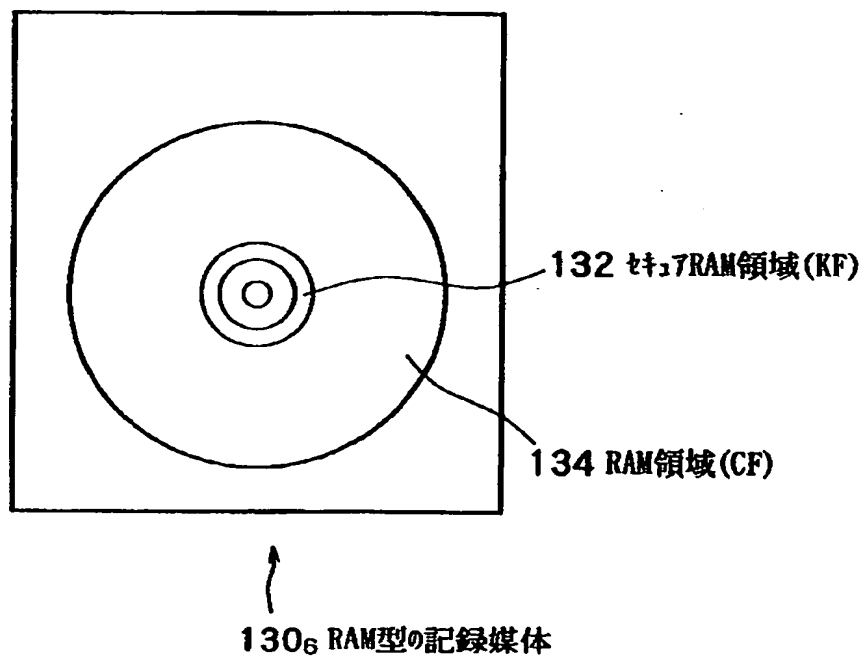
【図 1 4】



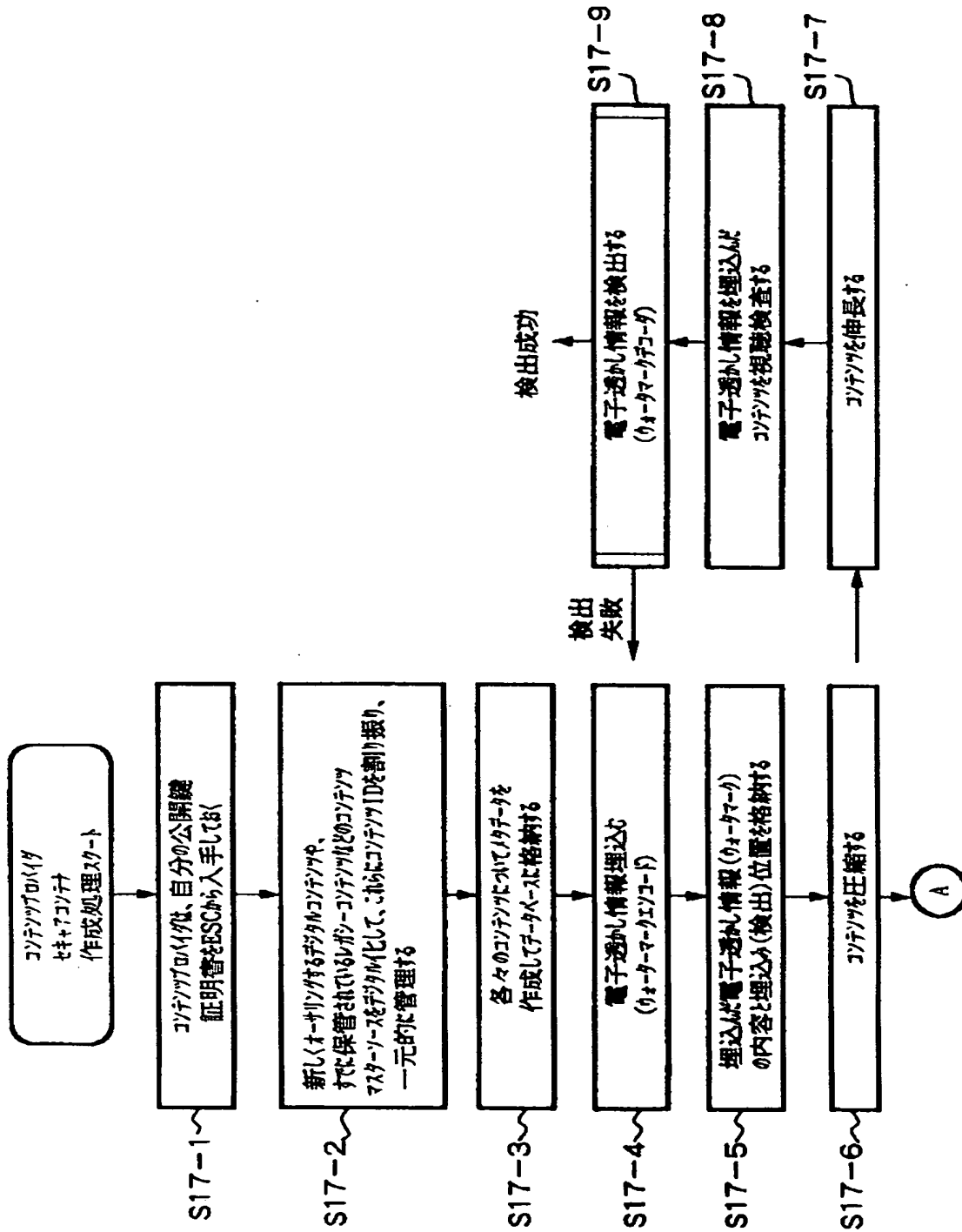
【図 1 5】



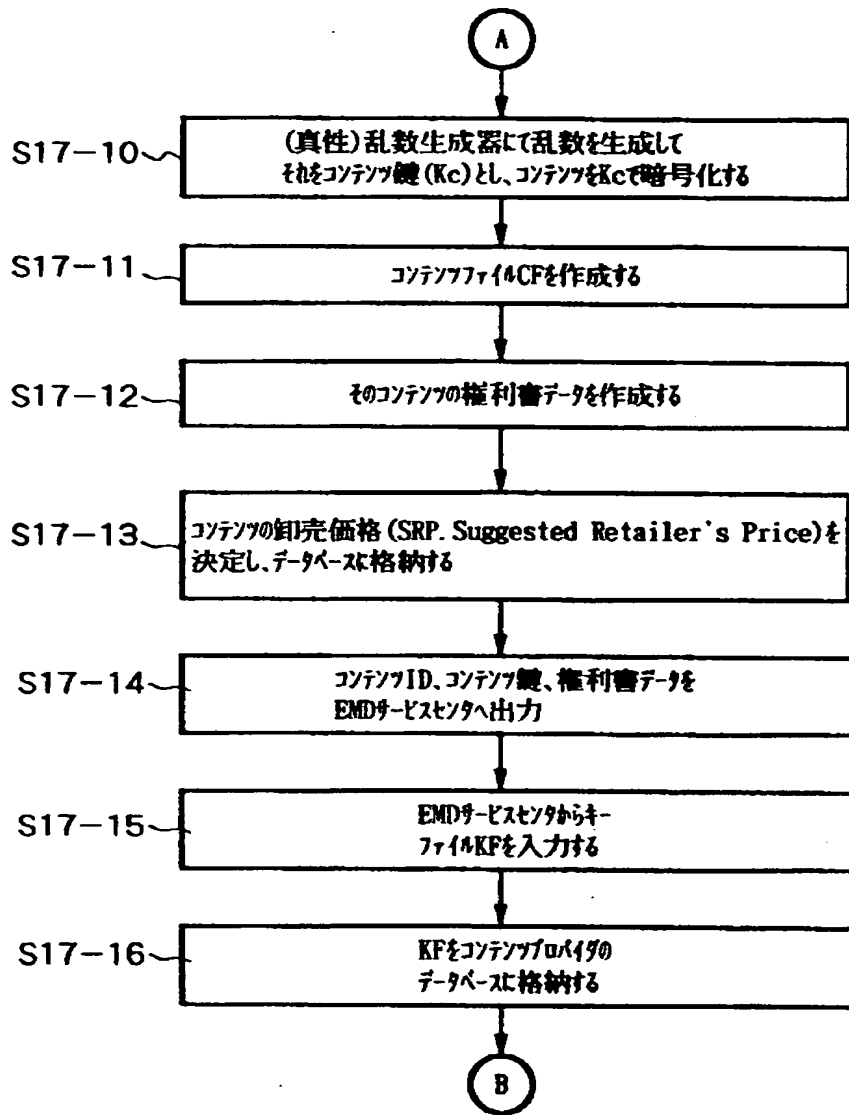
【図 1 6】



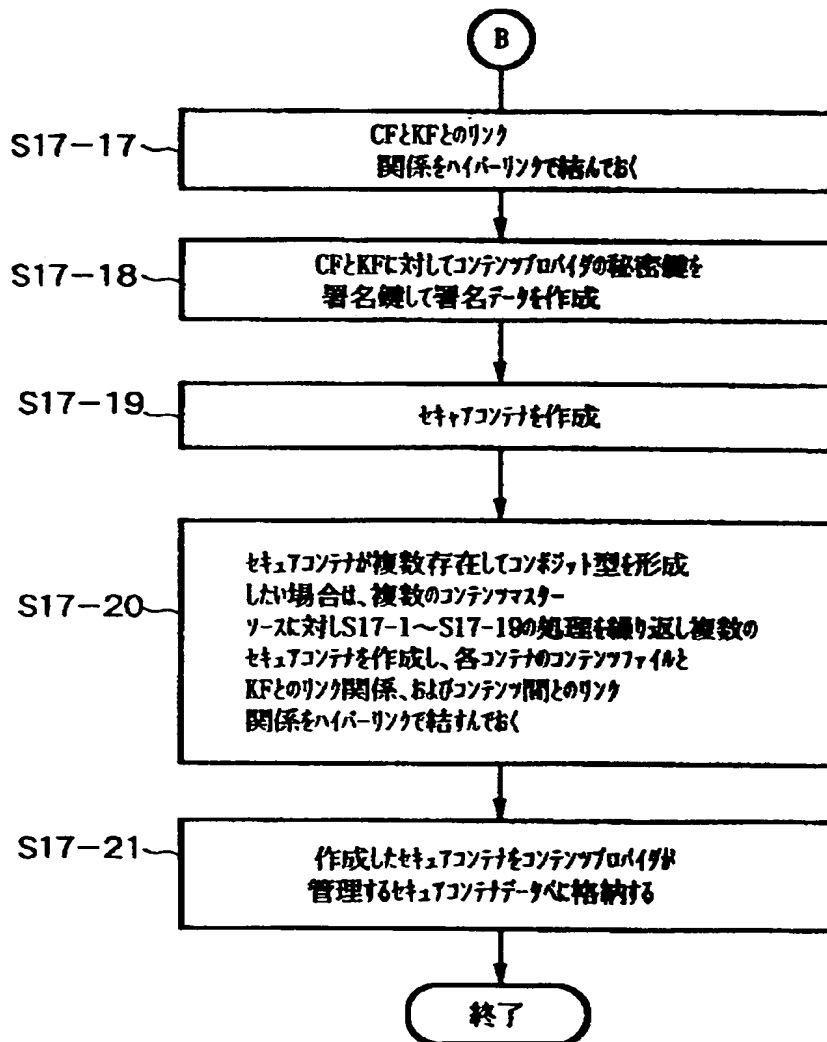
【図 1 7】



【図 1 8】



【図 1 9】



【図 2 0】

EMDサービス102の主な機能

ライセンス鍵データをコンテンツプロバイダよりSAMに供給

公開鍵証明書データCER_{CP}, CER_{SAM1}～CER_{SAM4}の発行

キーファイルKFの生成

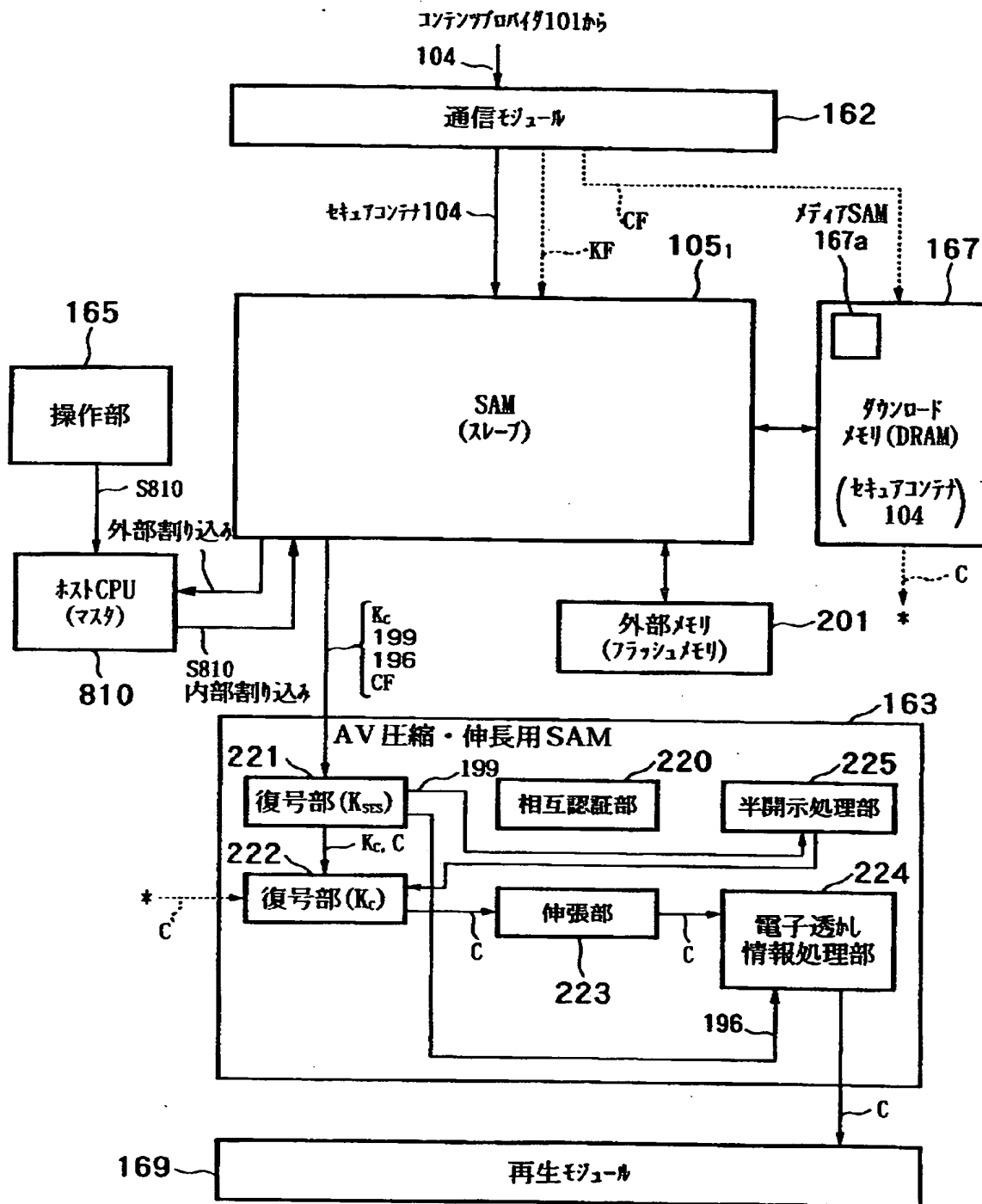
利用履歴データに基づいた決済処理(利益分配処理)

【図 2 1】

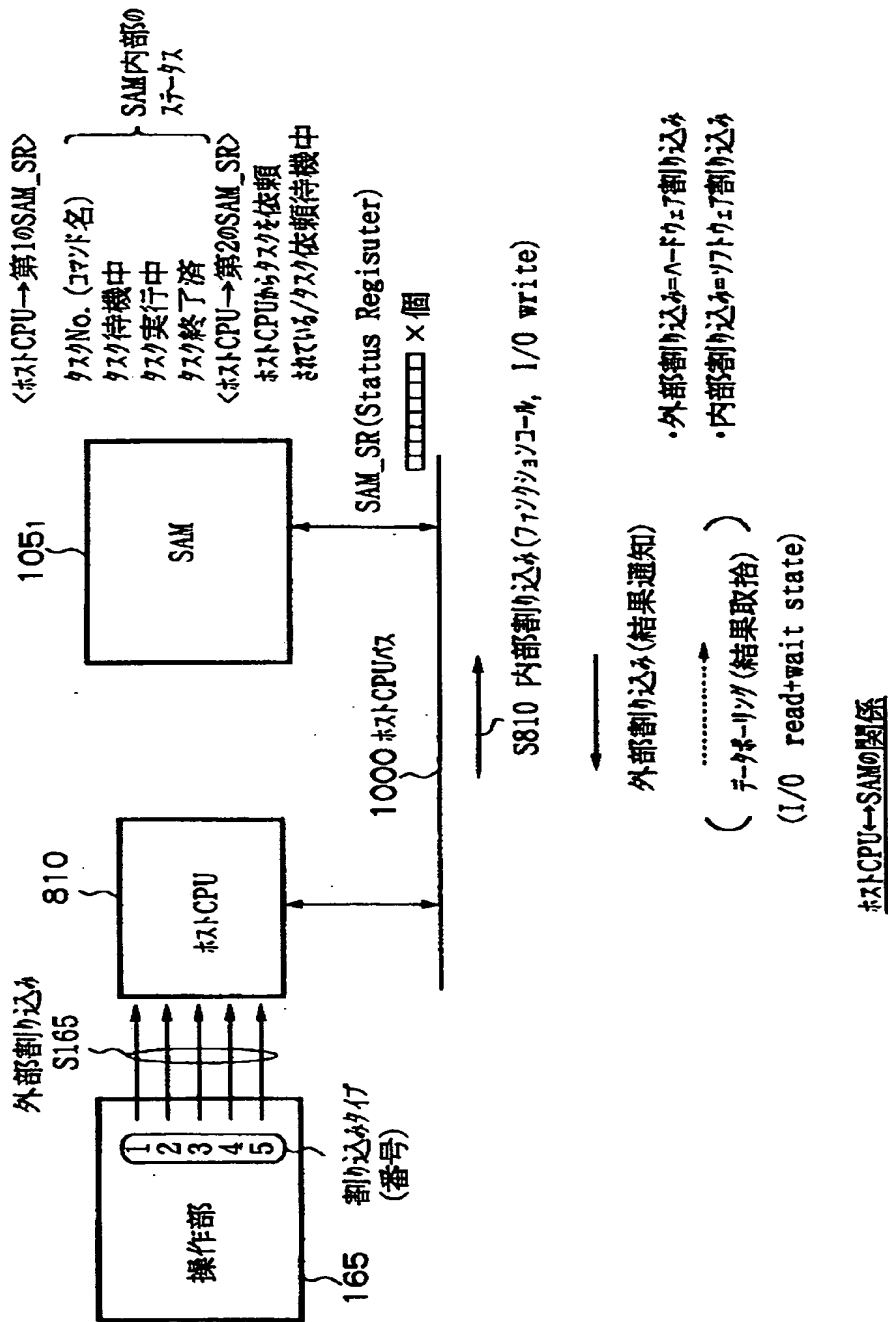
利用履歴データ108(308)

ESC_コンテンツID
CP_コンテンツID
(SP_コンテンツID)
ユーザID
ユーザ情報
SAM_ID
HNG_ID
ディスカント情報
トレーシング情報
(プライスタグデータPT)
CP_ID
(SP_ID)
紹介業者(ポータル:Portal)ID
ハードウェア提供者ID
Media_ID
コンポーネントID
ライセンス所有者の識別子LH_ID
ESC_ID

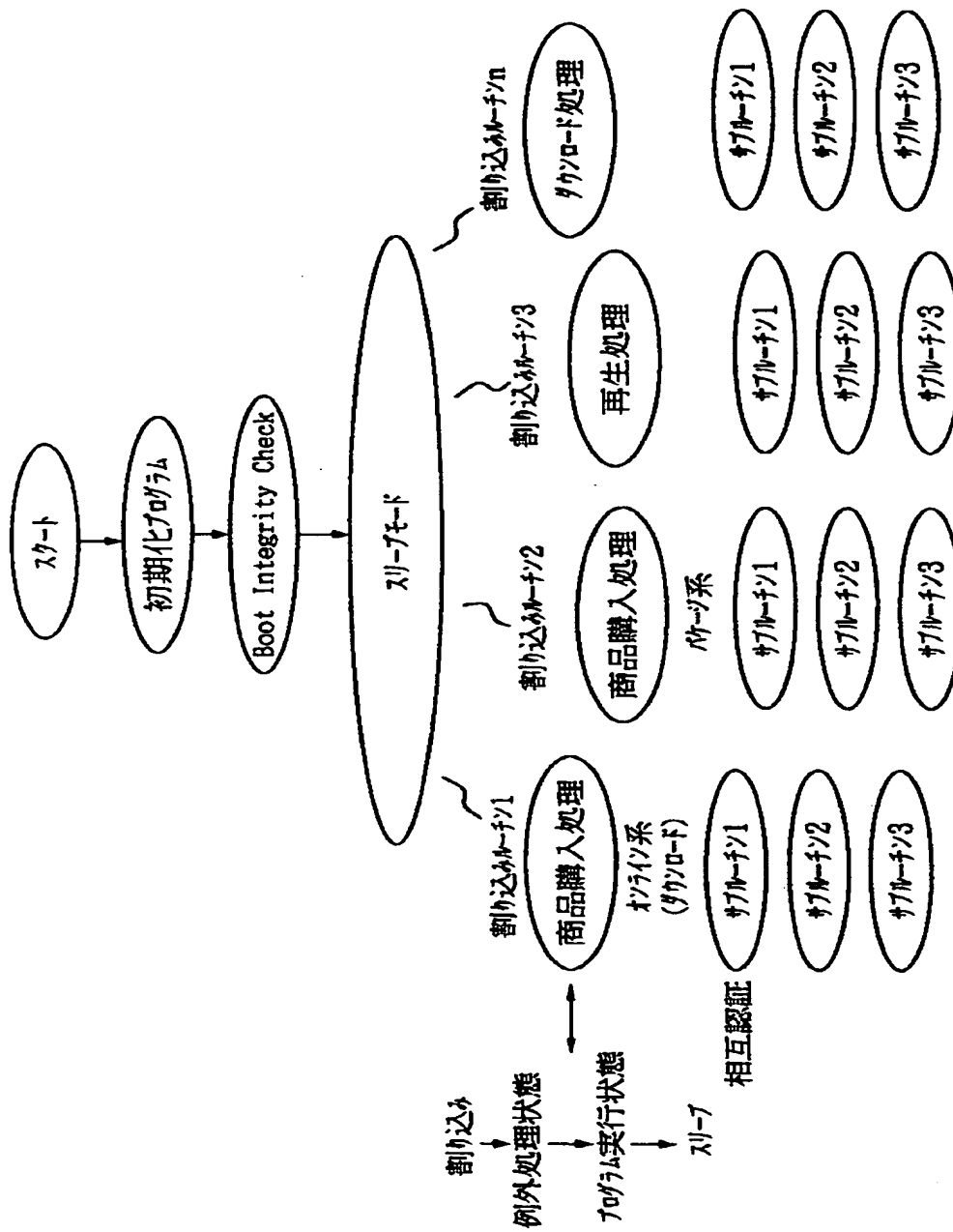
【図 2 2】



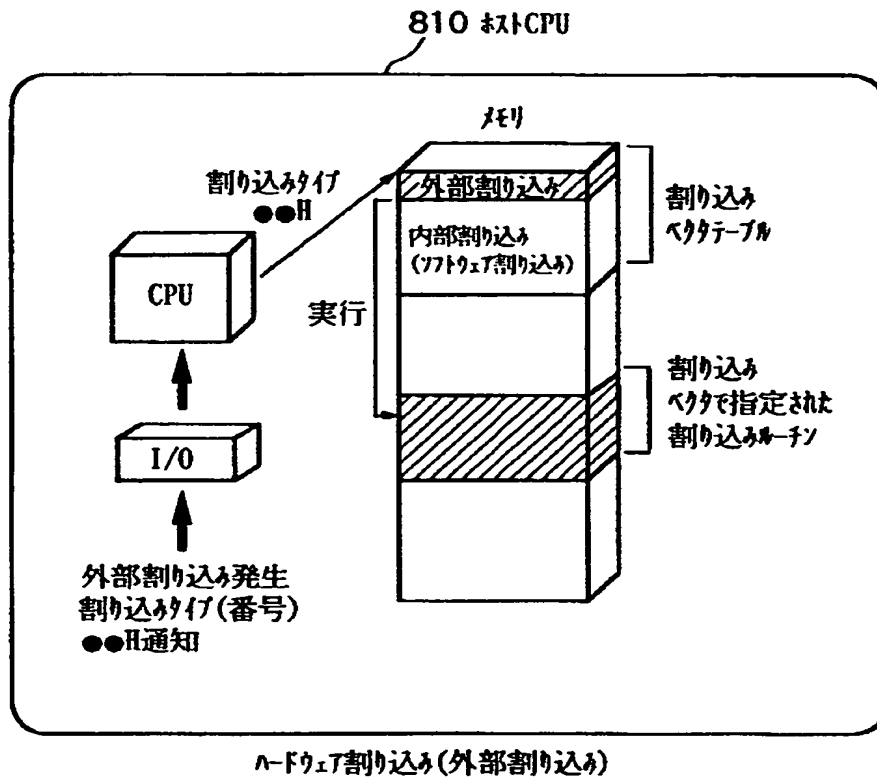
【図 2 3】



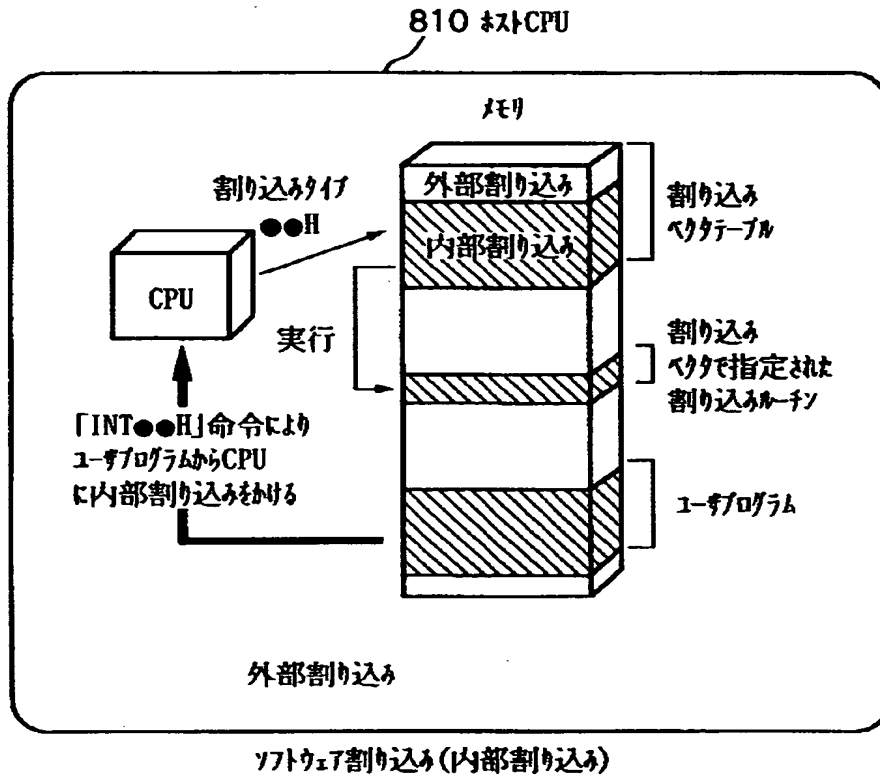
【図 2 4】



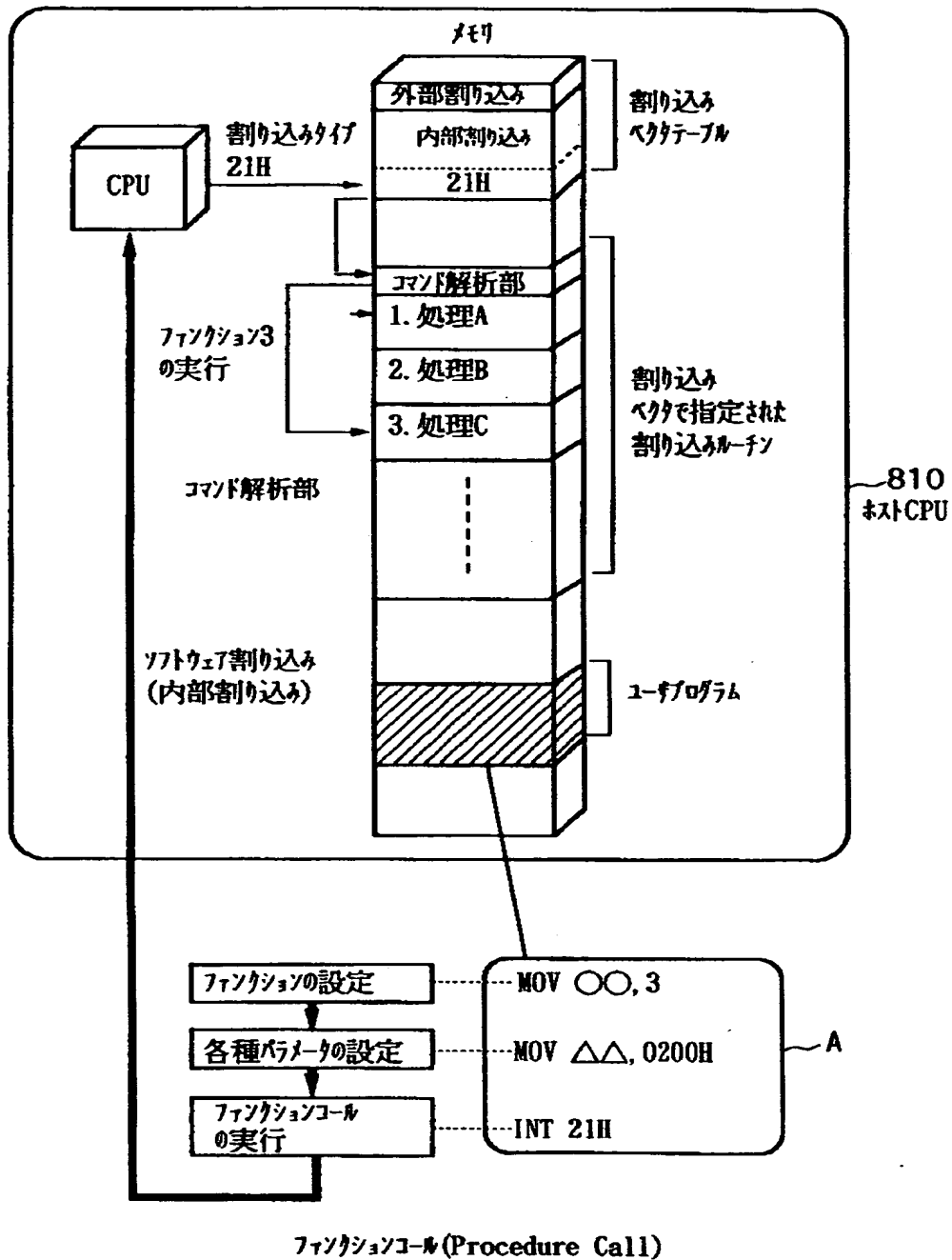
【図 2 5】



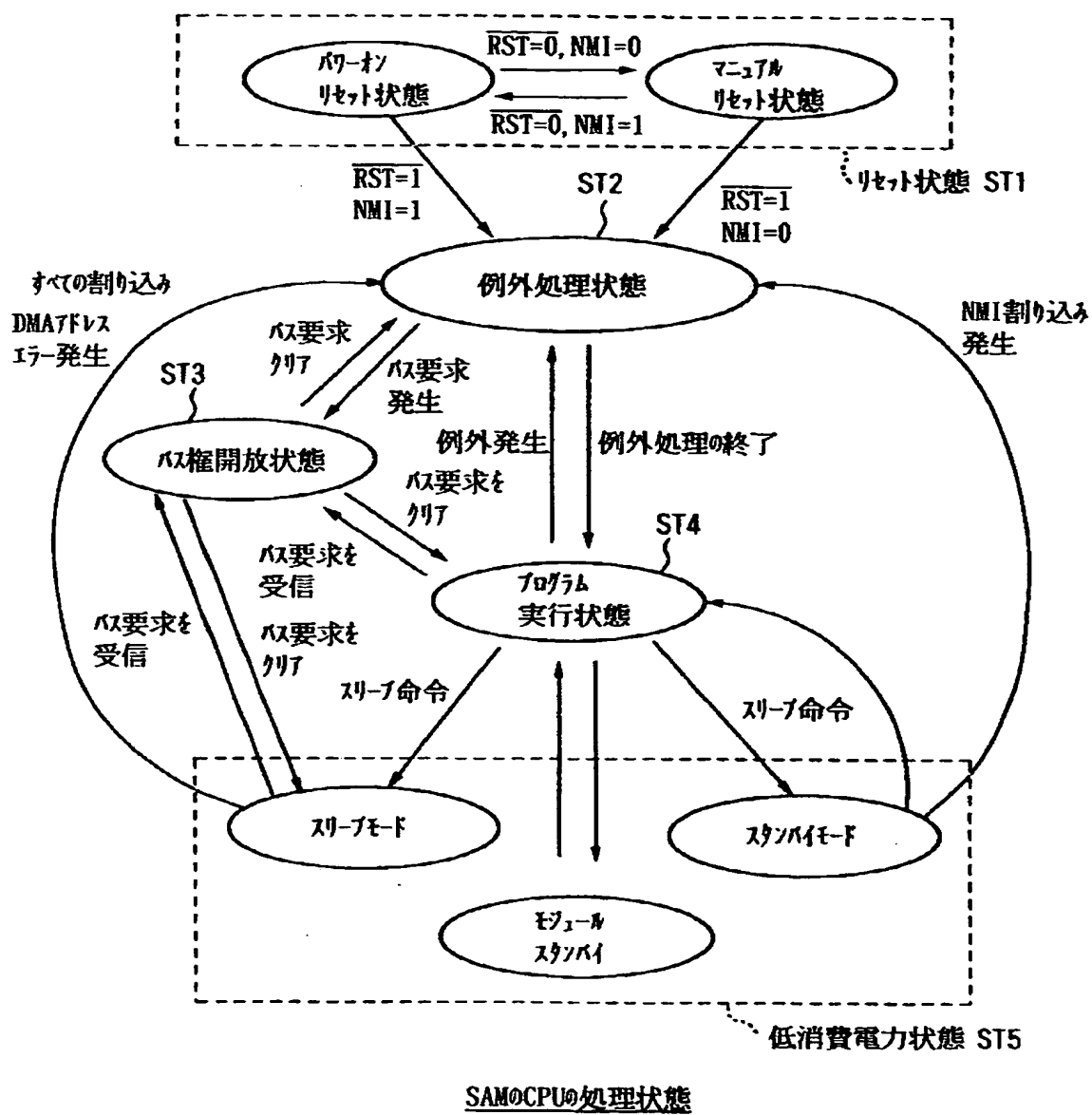
【図 2 6】



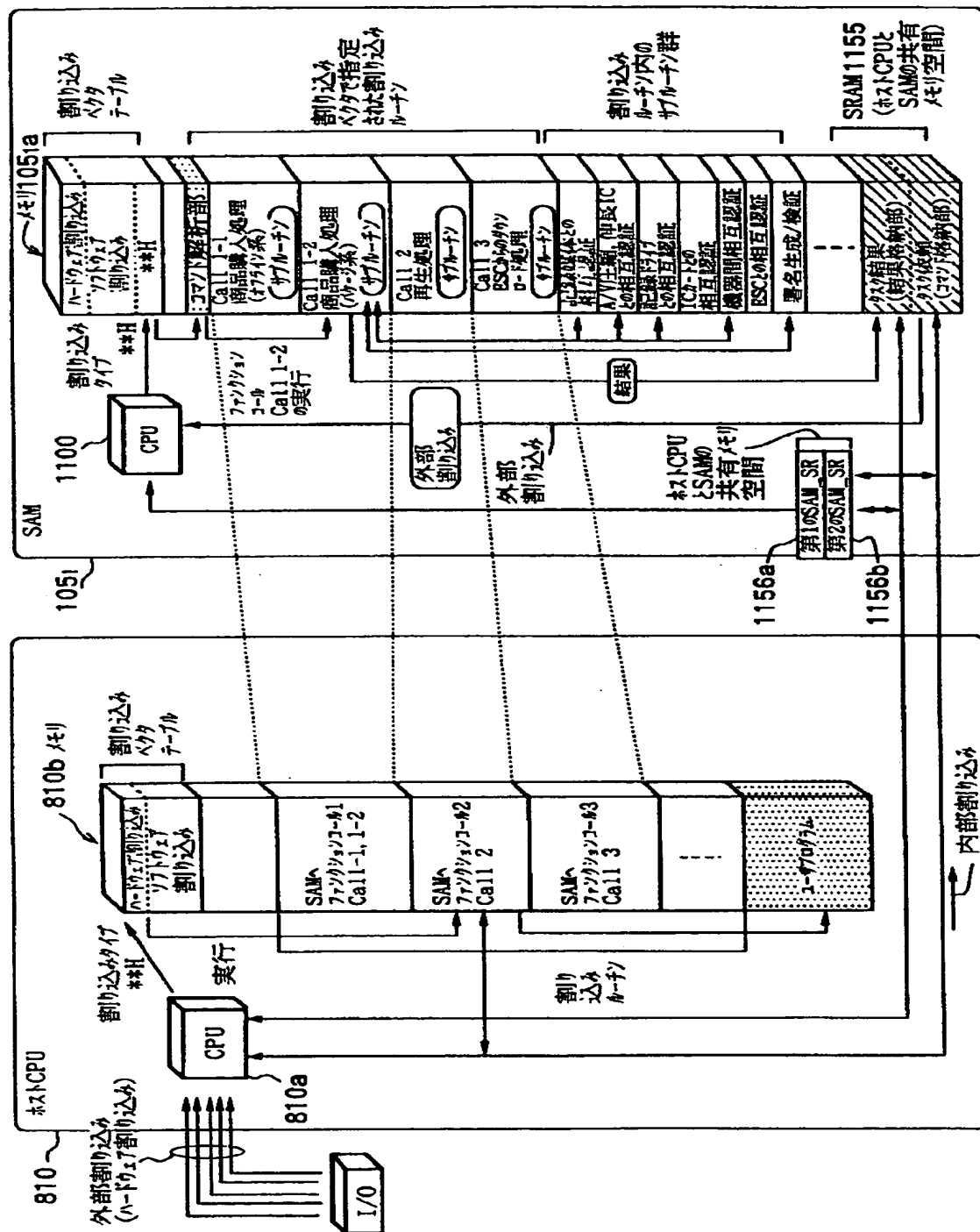
【図 27】



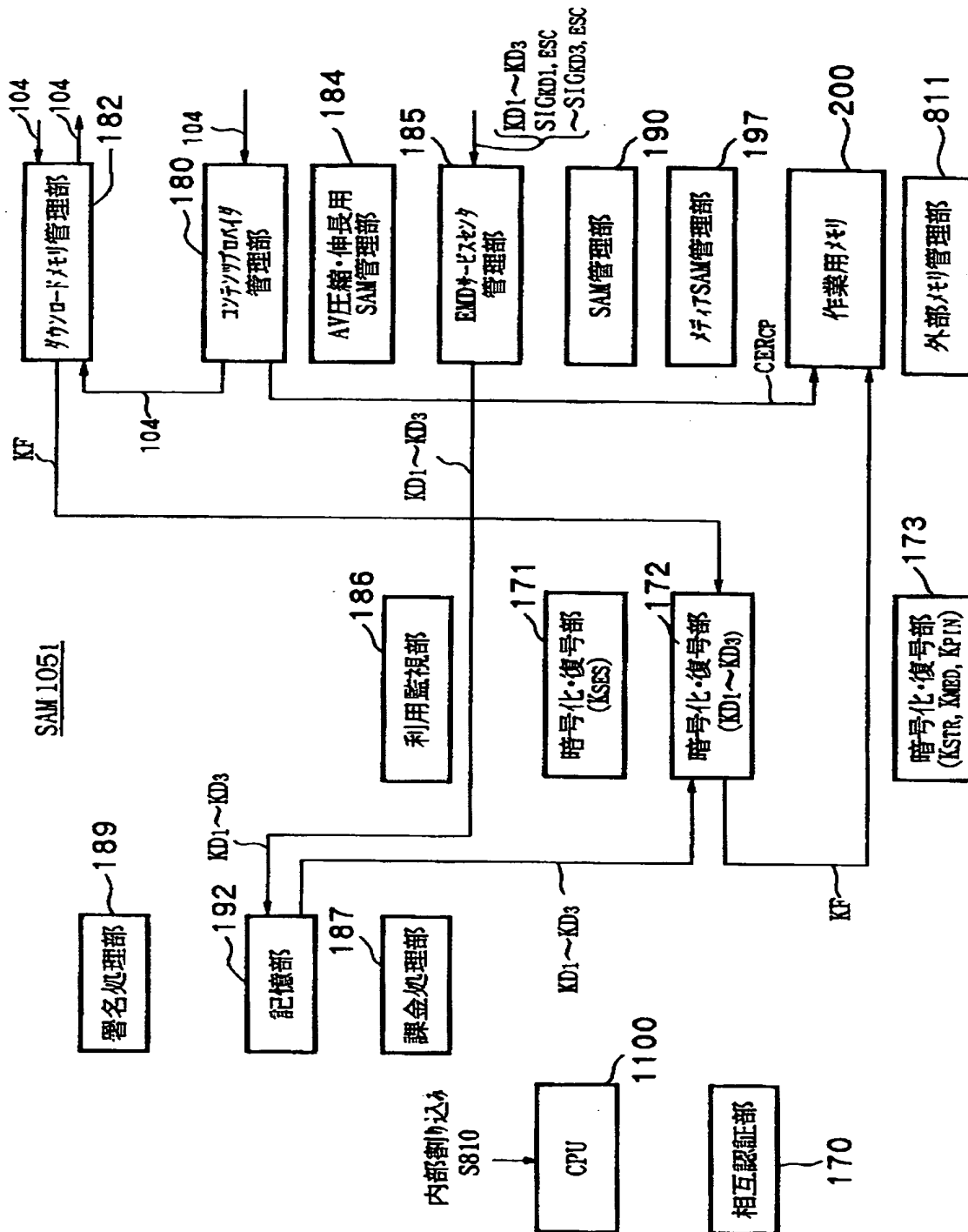
【图 28】



【图 29】



【図 30】



【図 3 1】

外部メモリ201に記憶されるデータ

利用履歴データ 108

SAM 登録リスト

(KF:ダウンロードメモリにデータ SAM が無い場合)

【図 3 2】

作業用メモリ200に記憶されるデータ

コンテンツ鍵データKc

権利書データ(UCP) 106

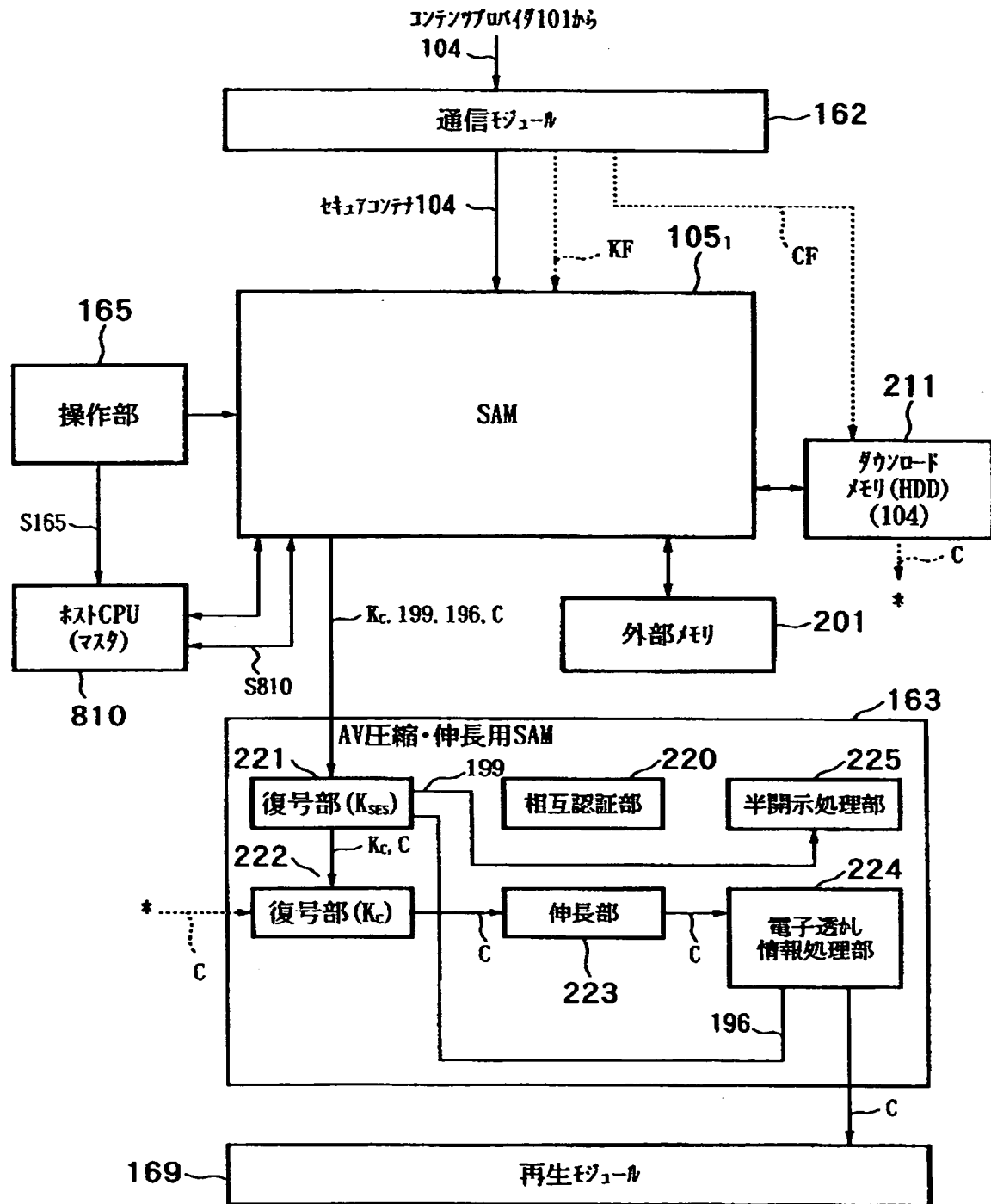
記憶部(フラッシュメモリ) 192のロック鍵データK_{loc}

コンテンツプロバイダ101の公開鍵証明書CER_{cp}

利用制御データ(UCS) 166

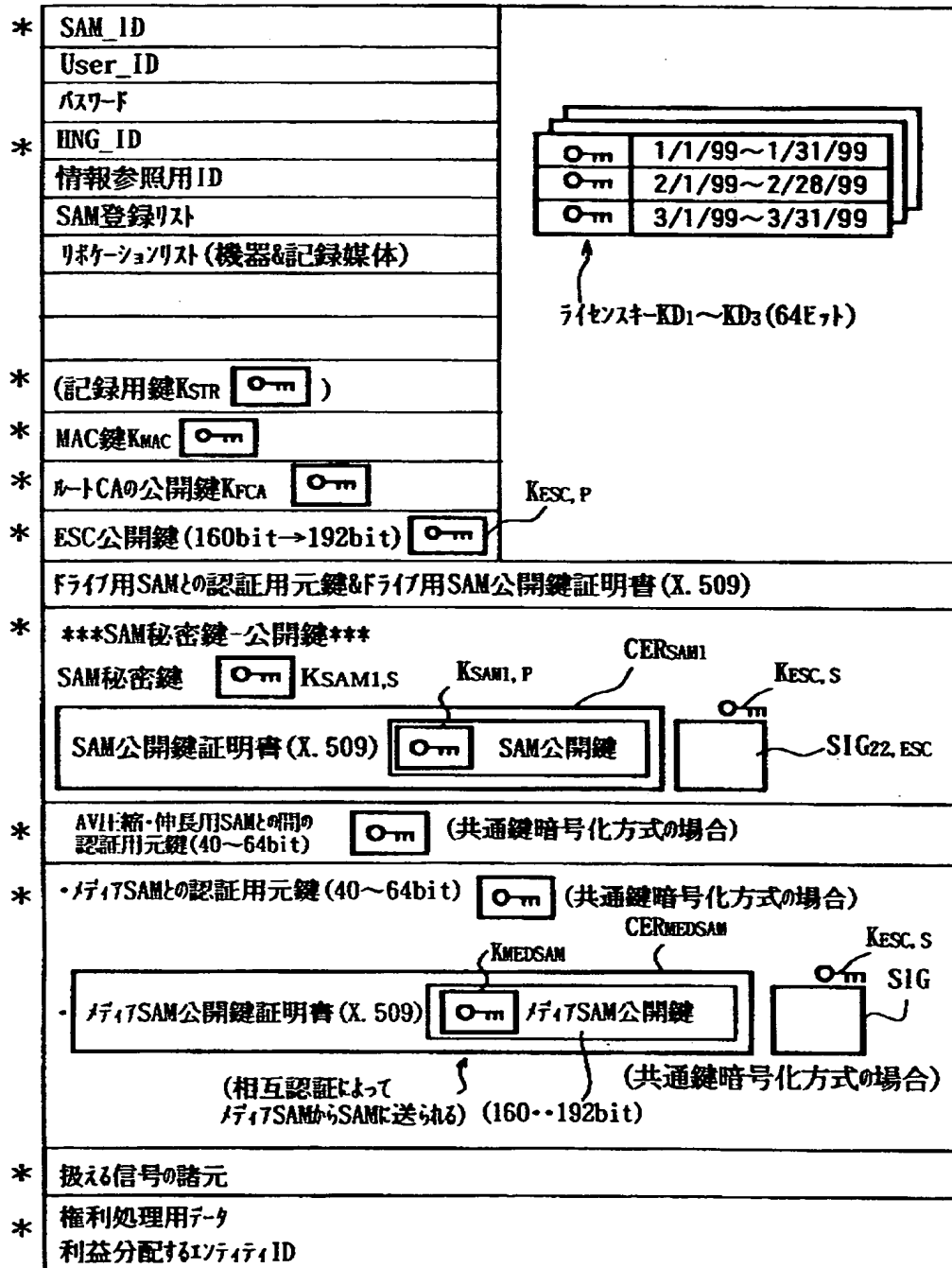
SAMプログラム・ダウンロード・コンテンツSD₁～SD₃

【図 3 3】

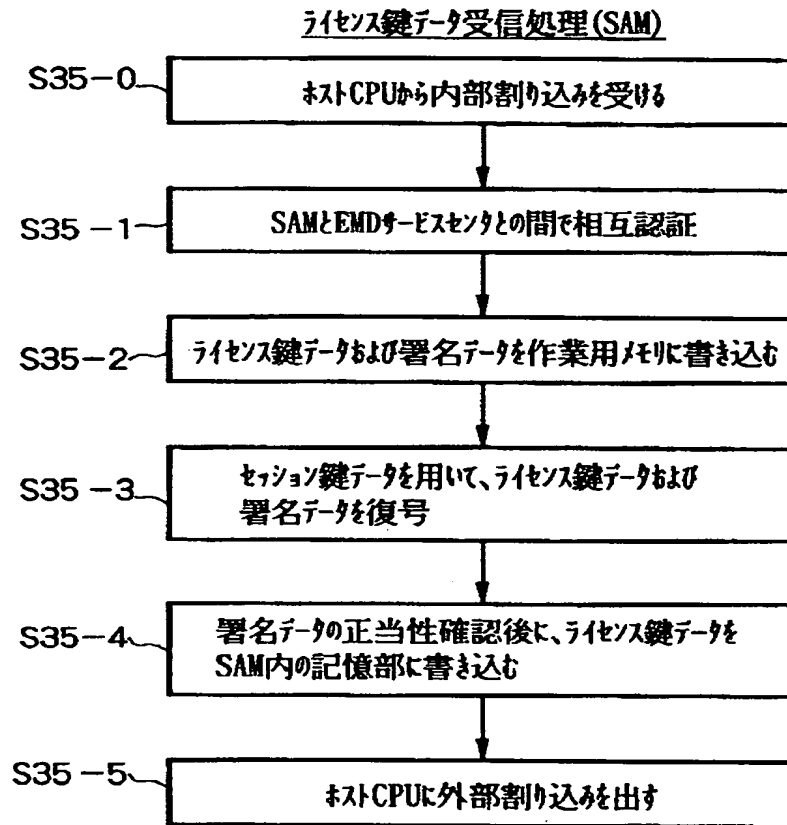


【図 3 4】

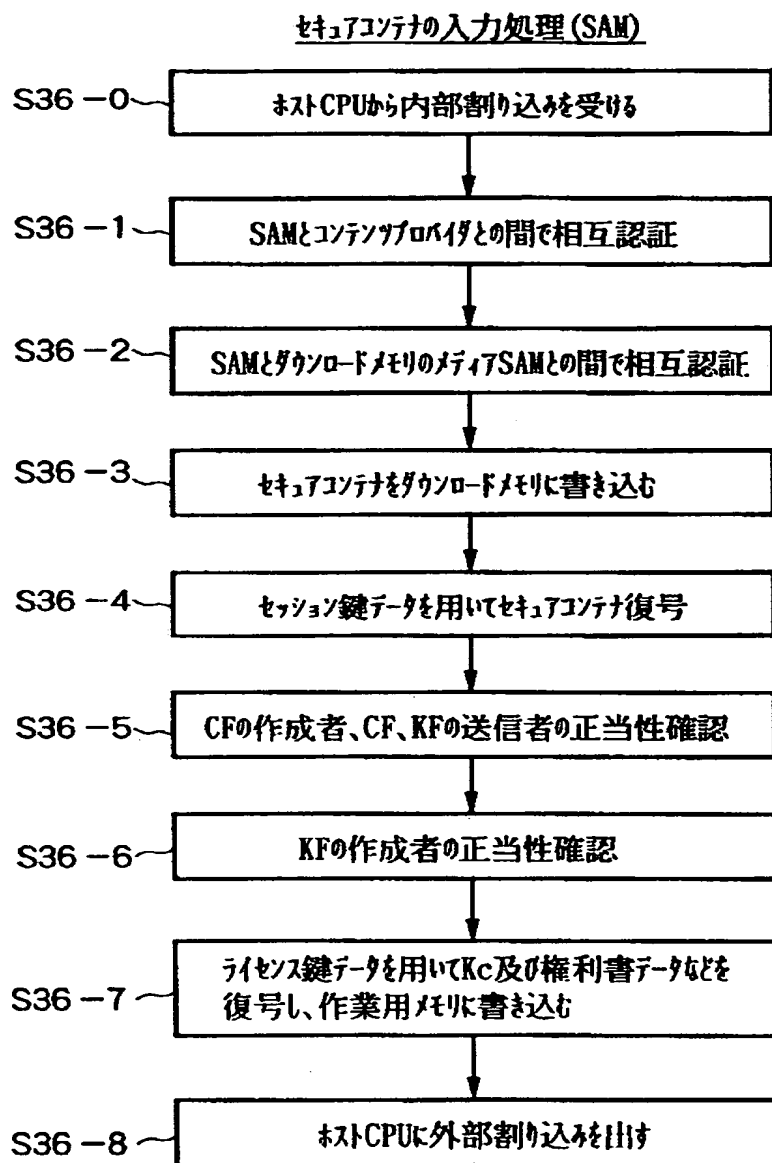
記憶部192に記憶されるデータ



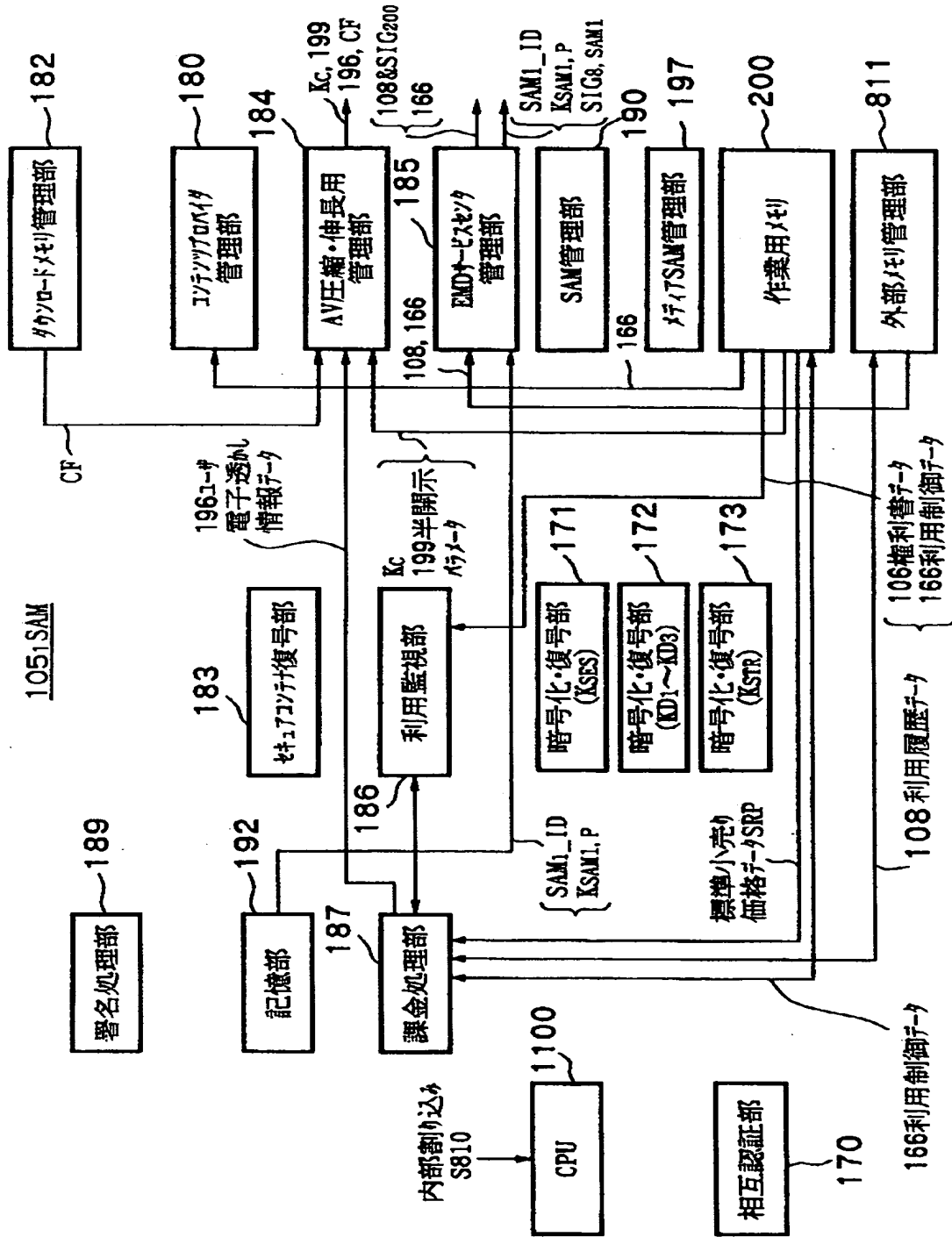
【図 3 5】



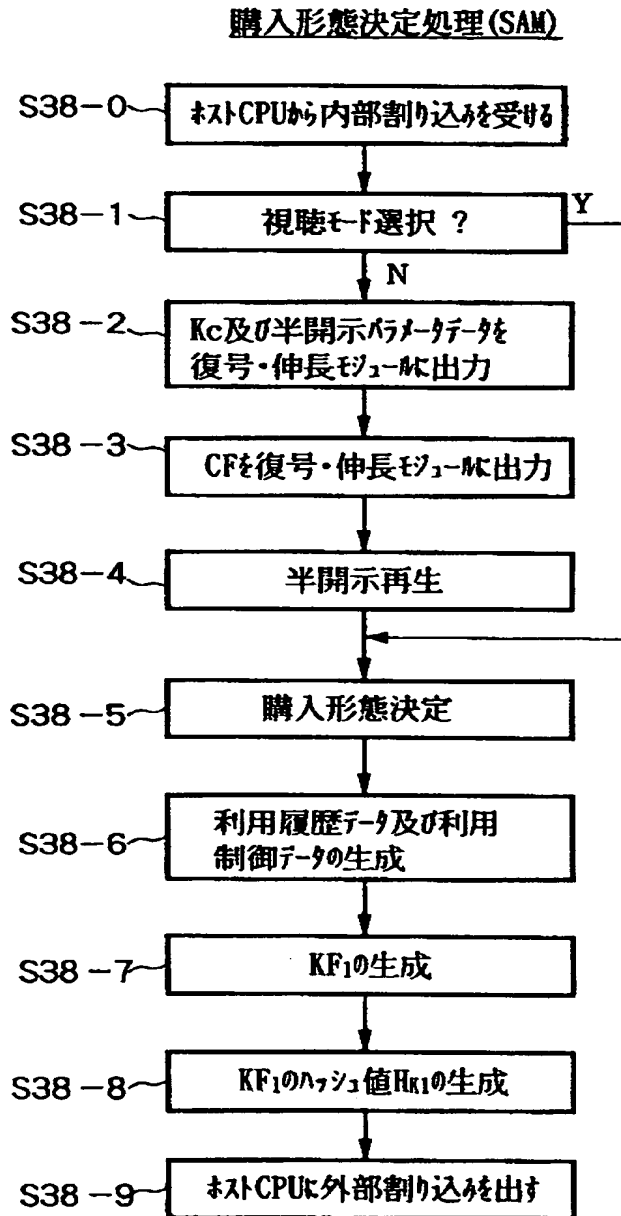
【図 3 6】



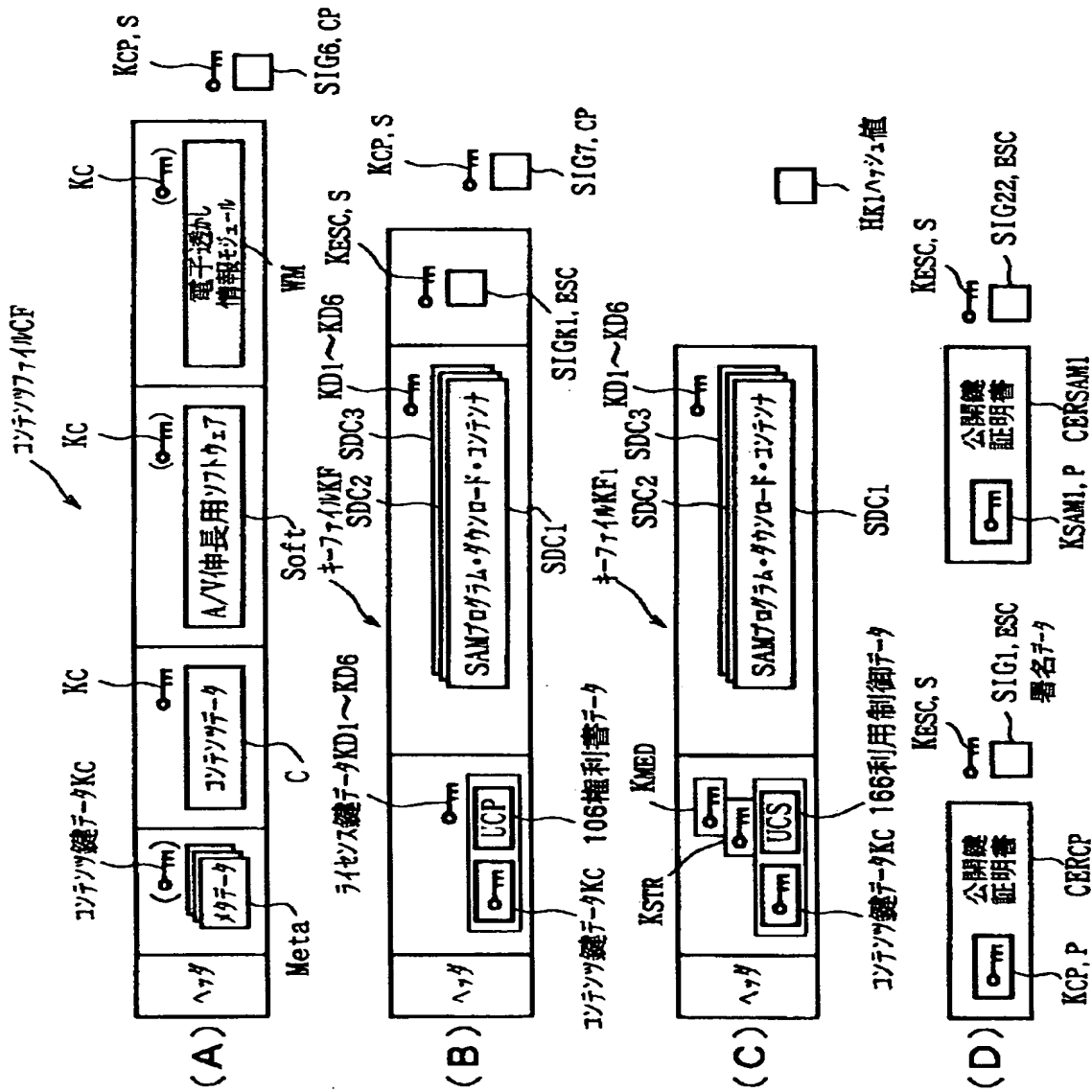
【図 3 7】



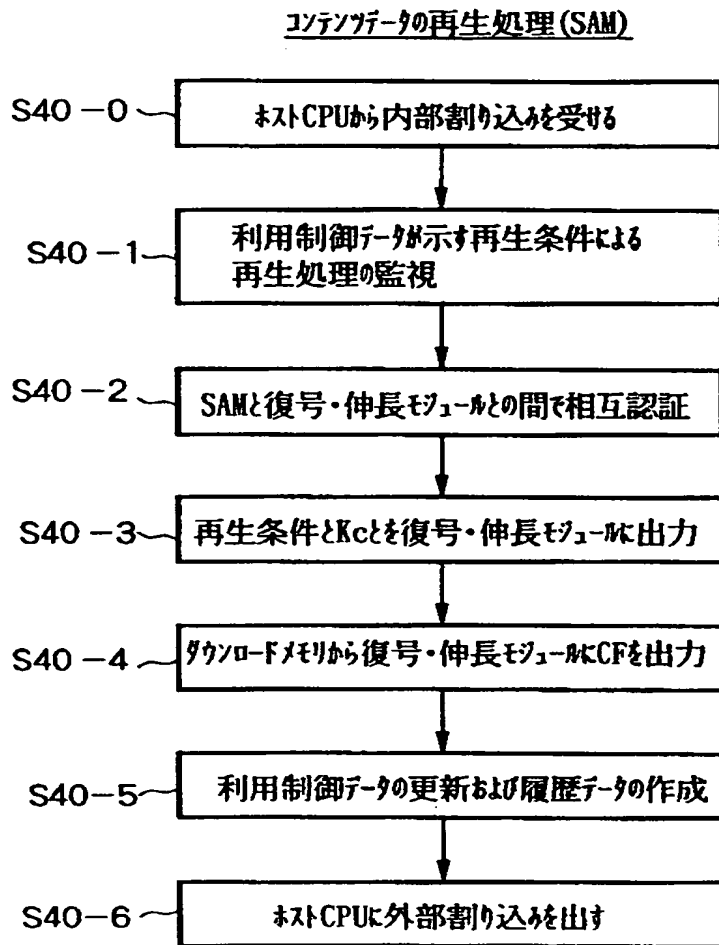
【図 3 8】



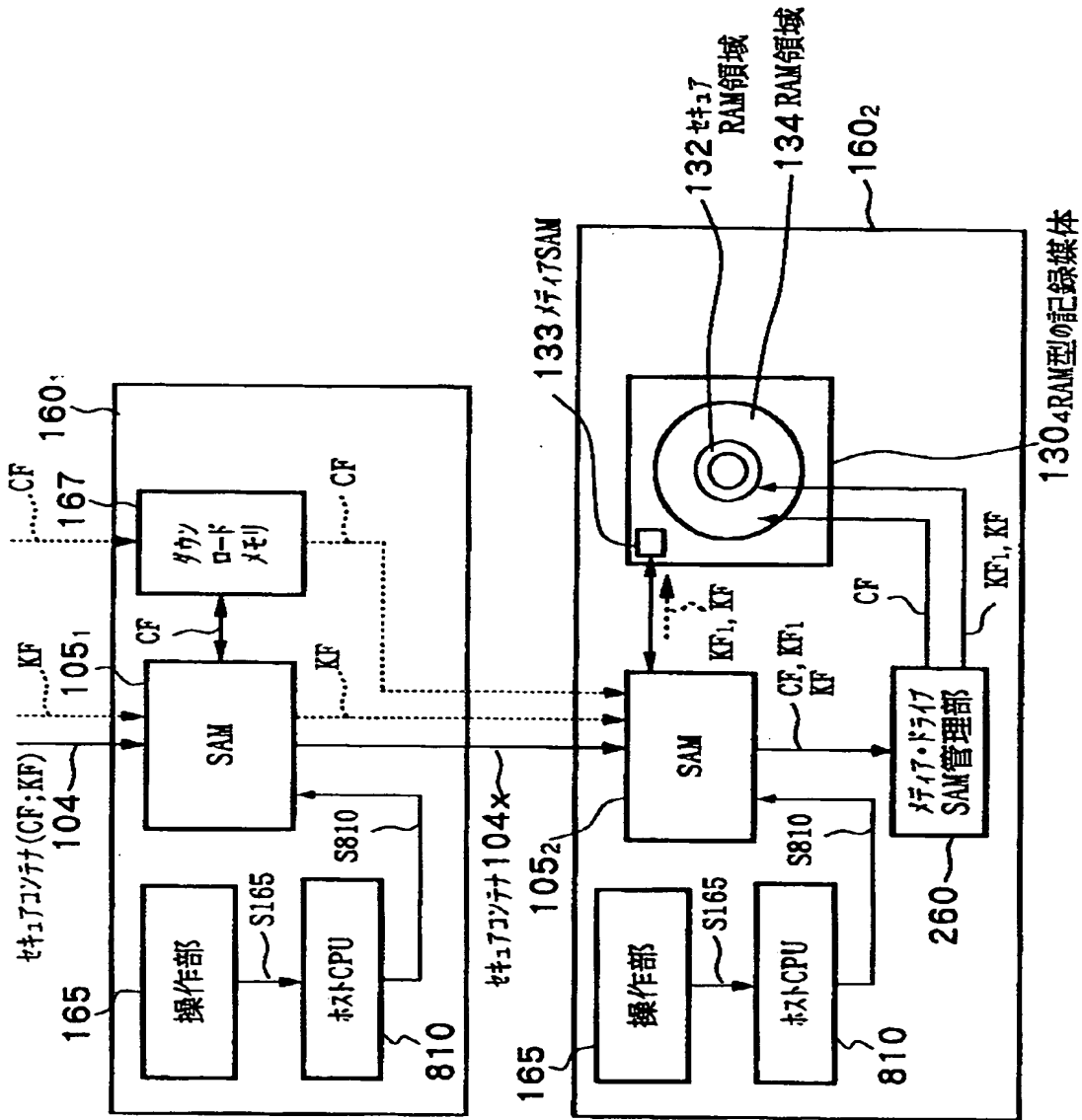
【図 3 9】



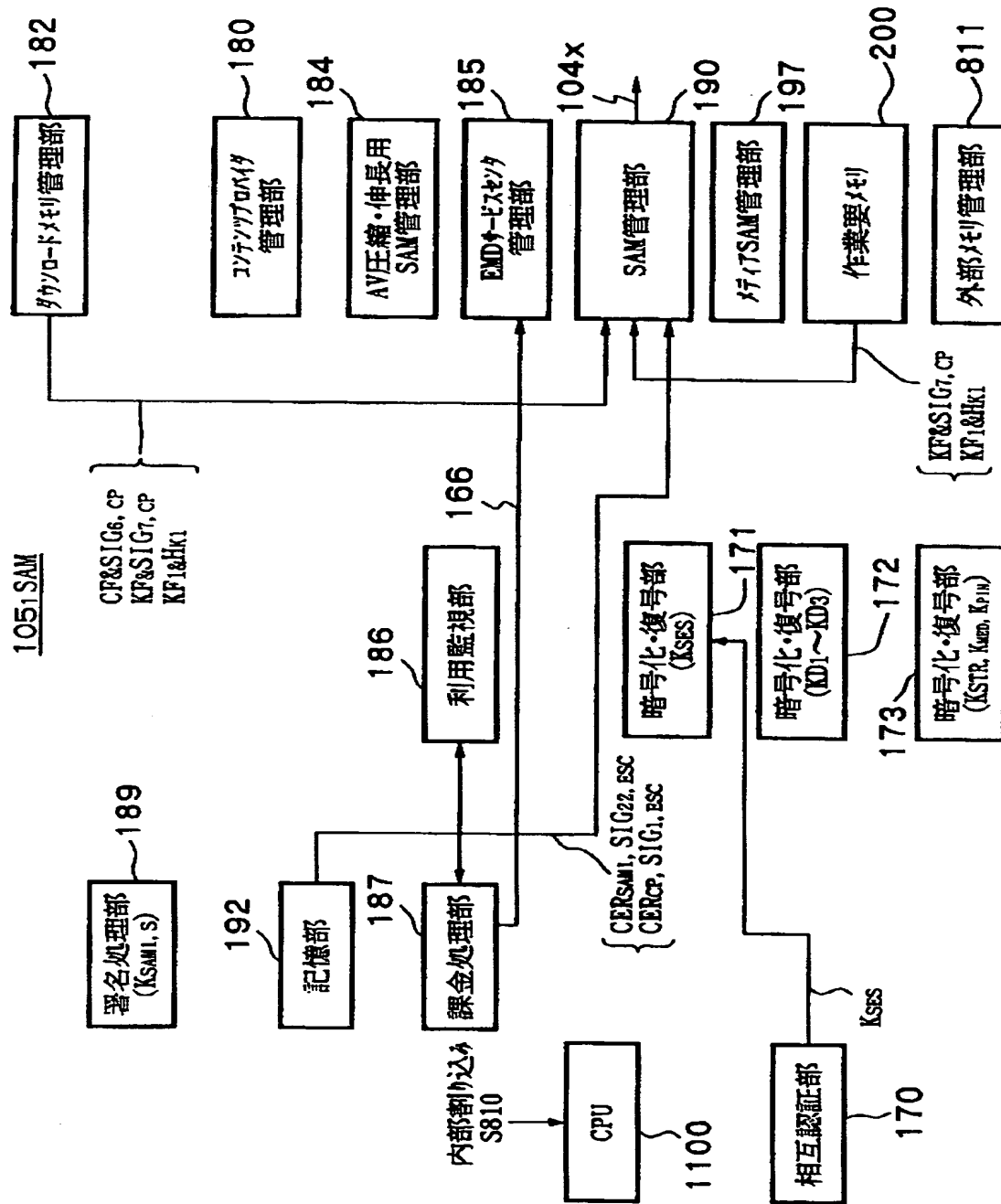
【図 4 0】



【図 4 1】

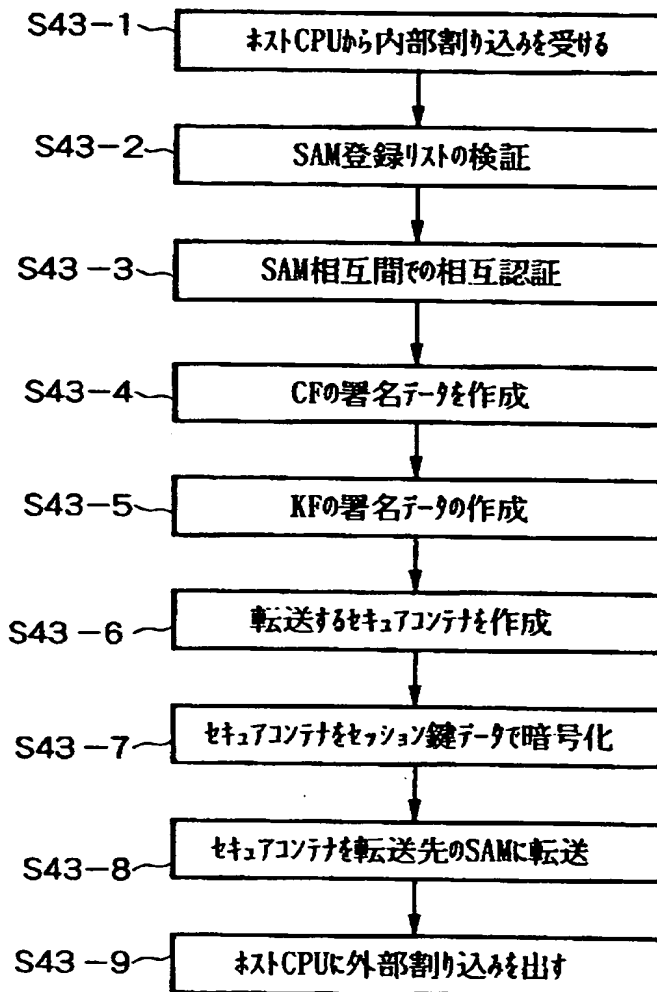


【図 4 2】

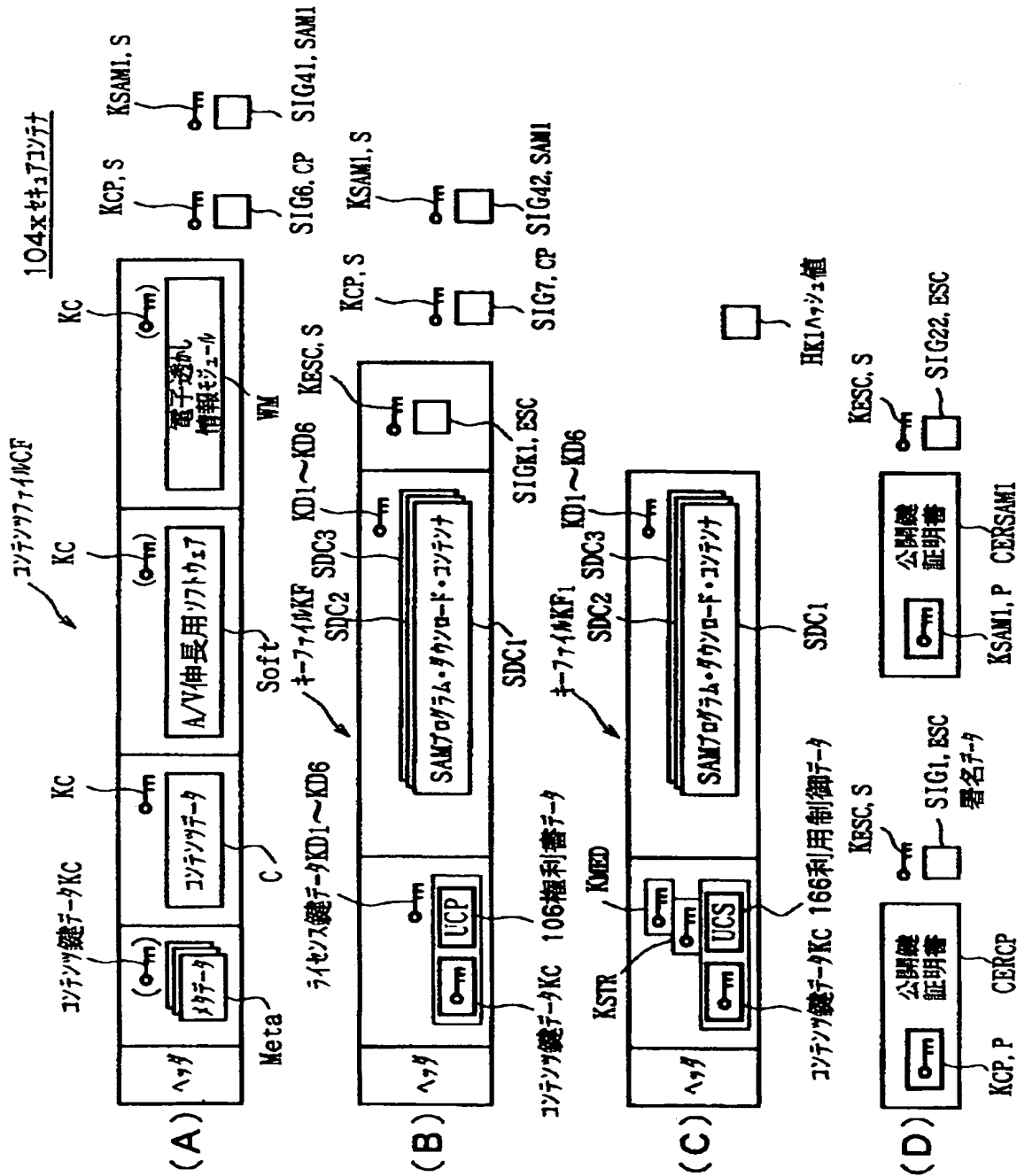


【図 4 3】

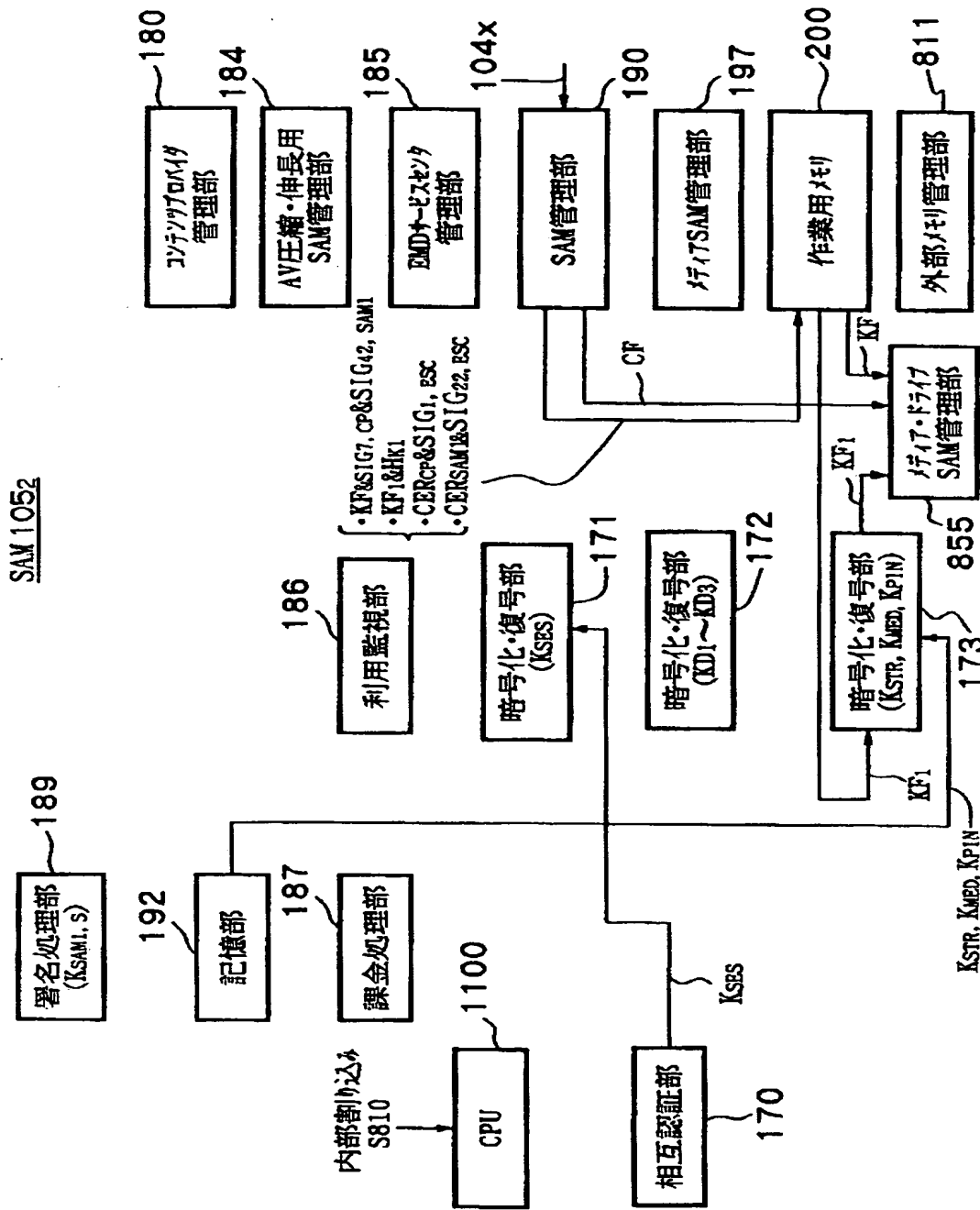
一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送元のSAMの処理



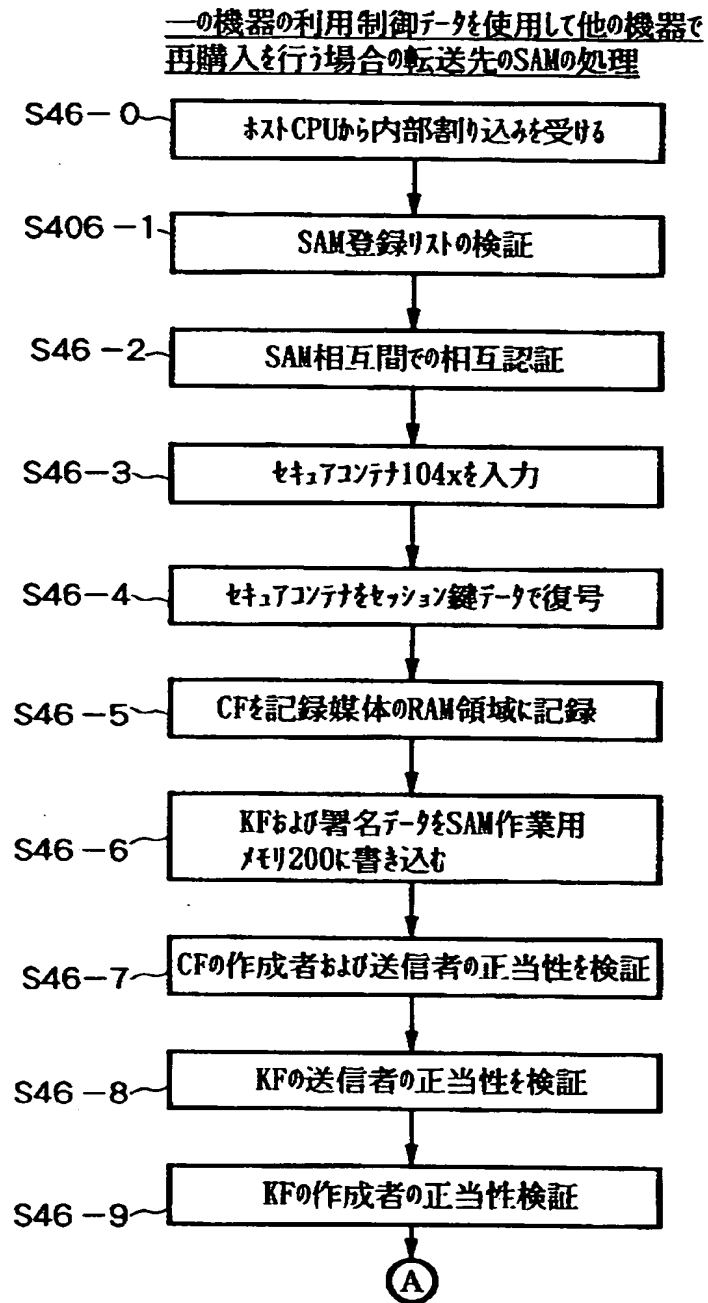
【図 4 4】



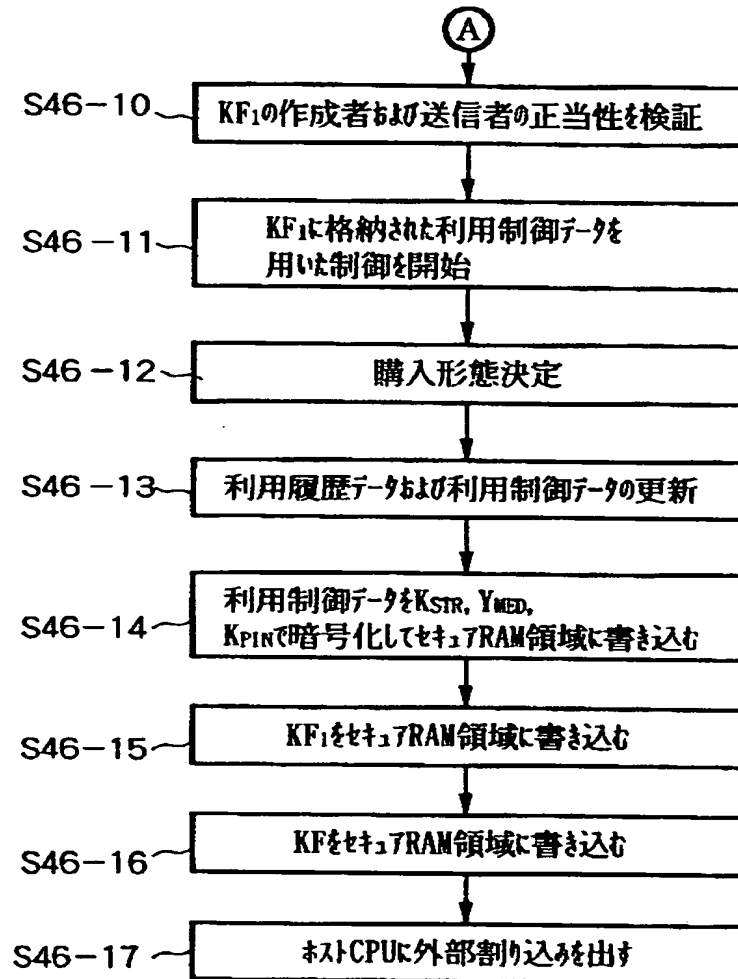
【図 4 5】



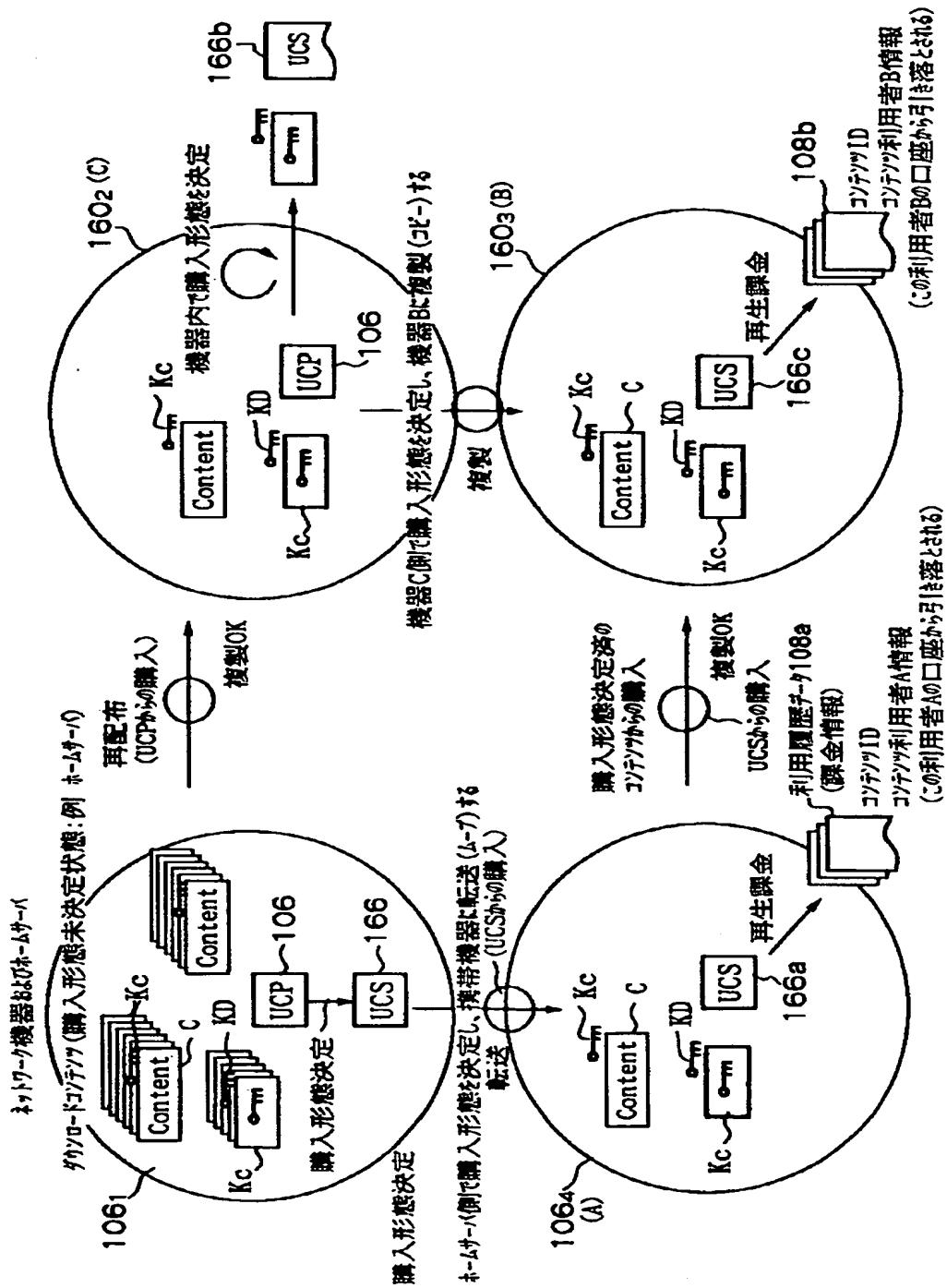
【図 4 6】



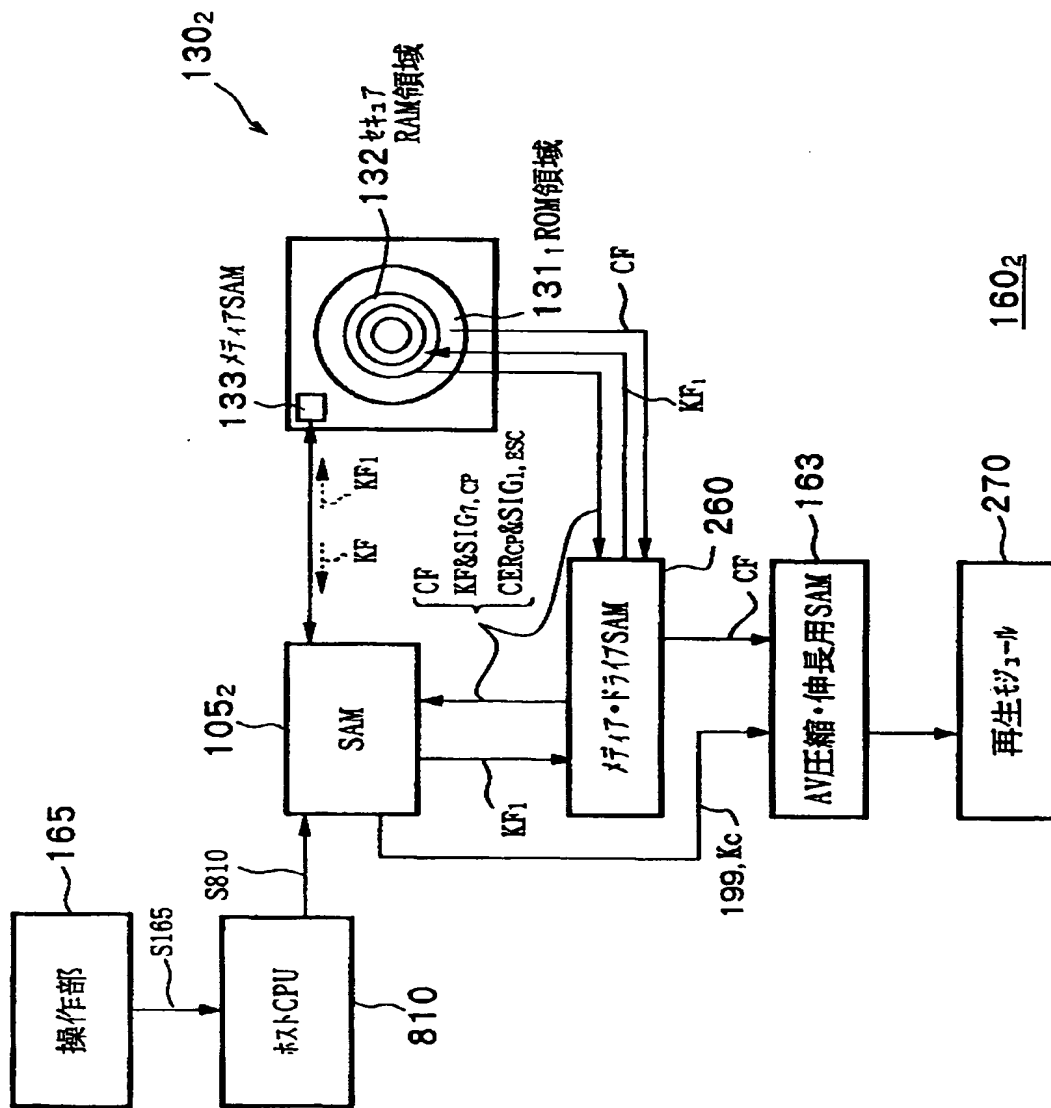
【図 4 7】



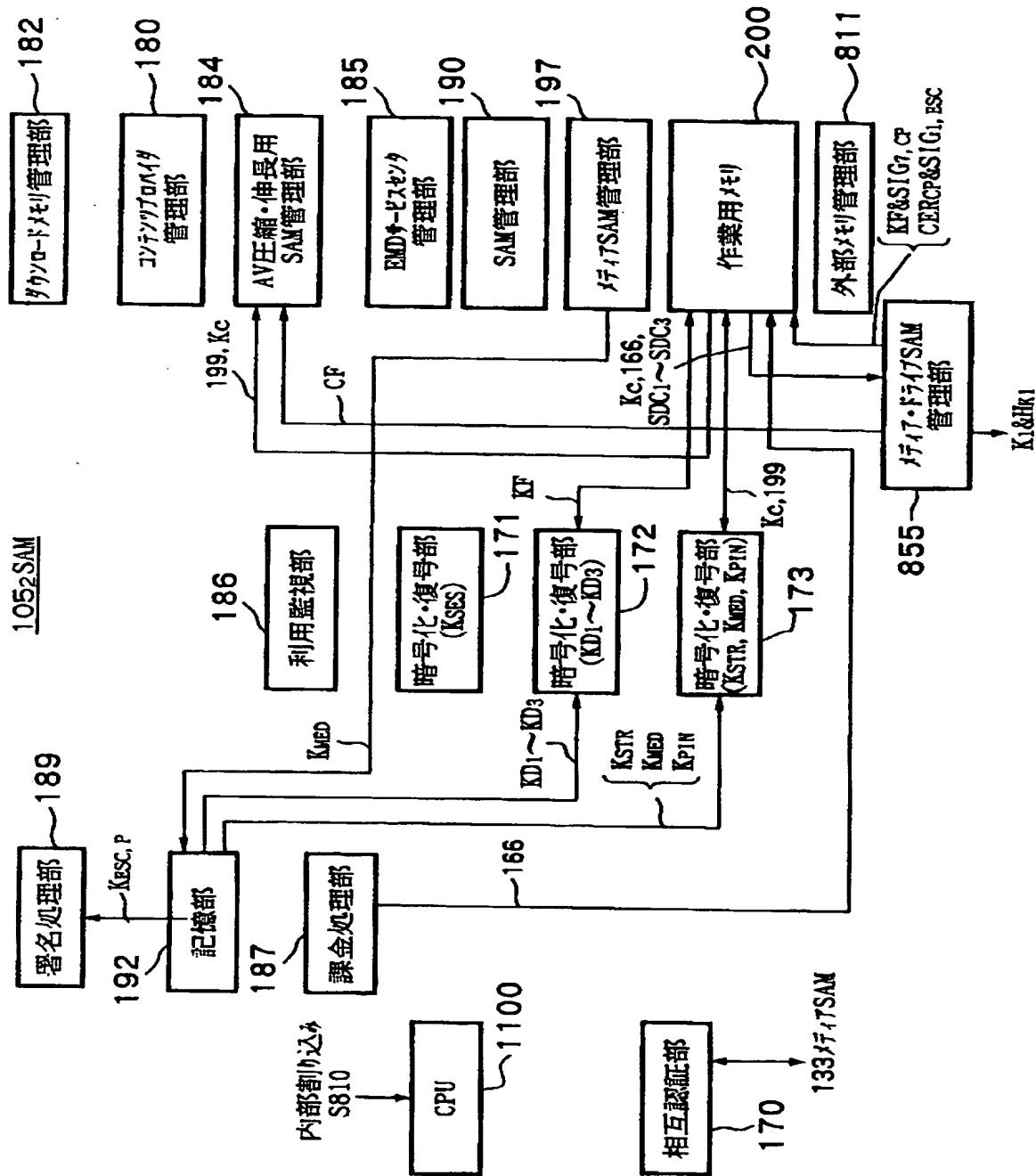
【図 4 8】



【図 4 9】

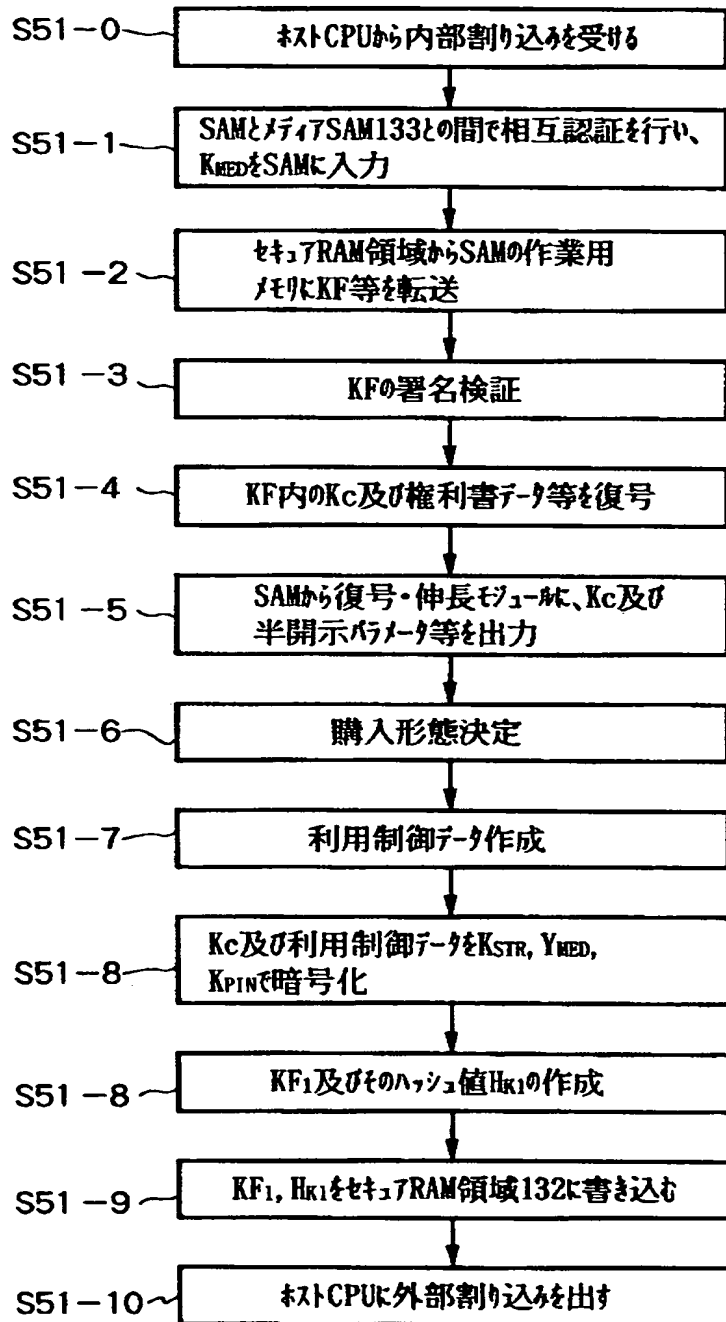


【図 50】

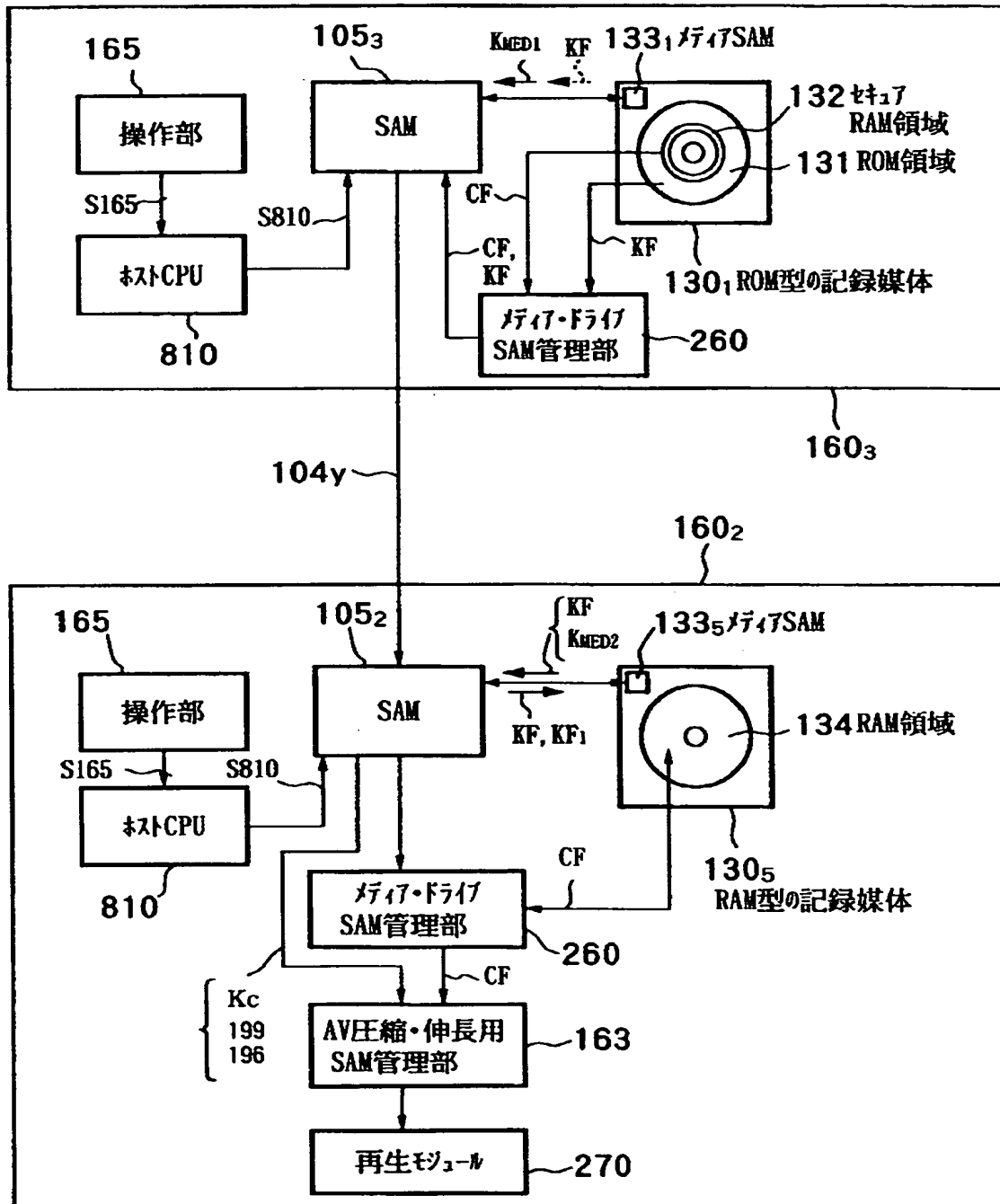


【図 5 1】

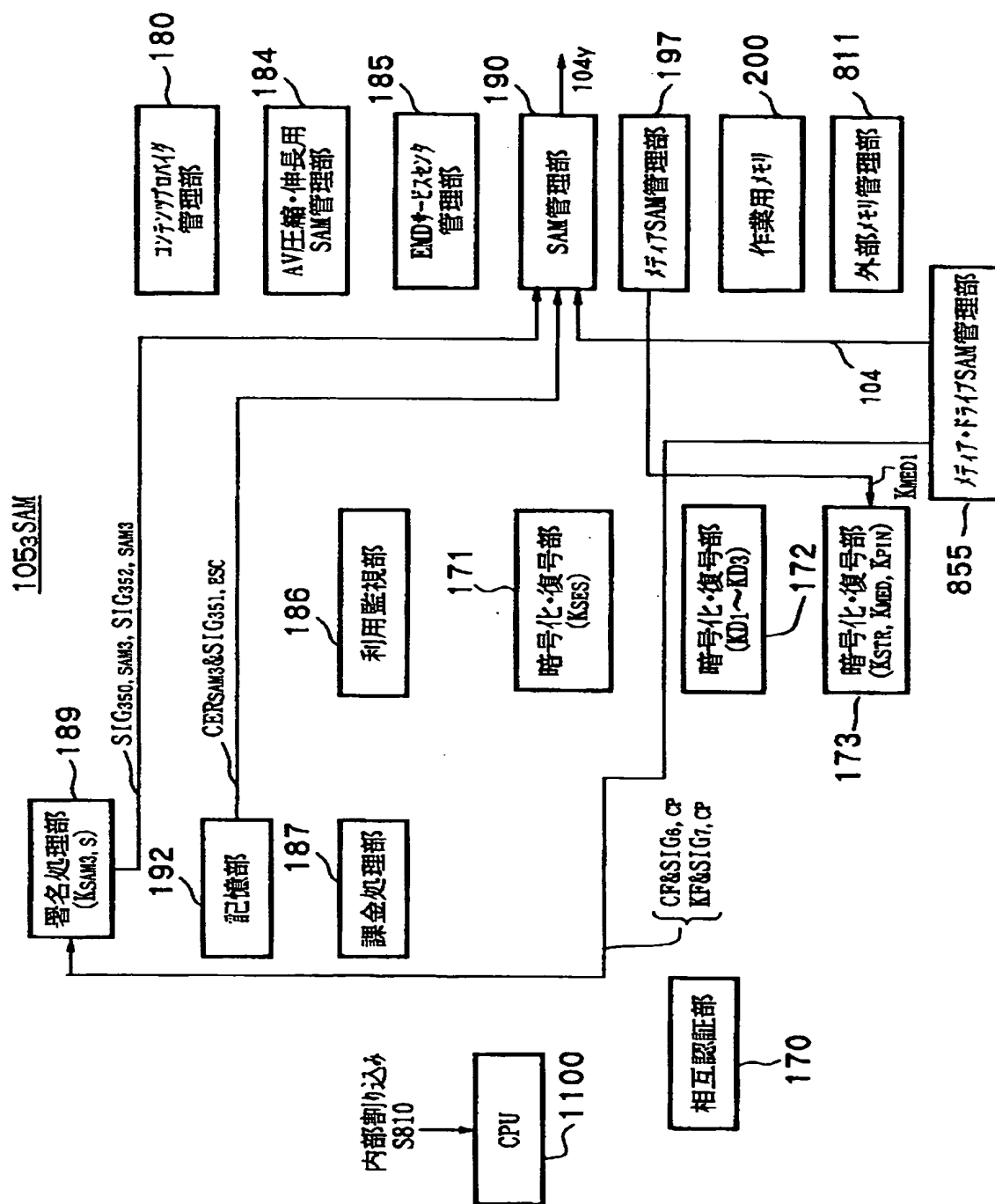
ROM型の記録媒体のコンテンツデータの購入形態決定処理



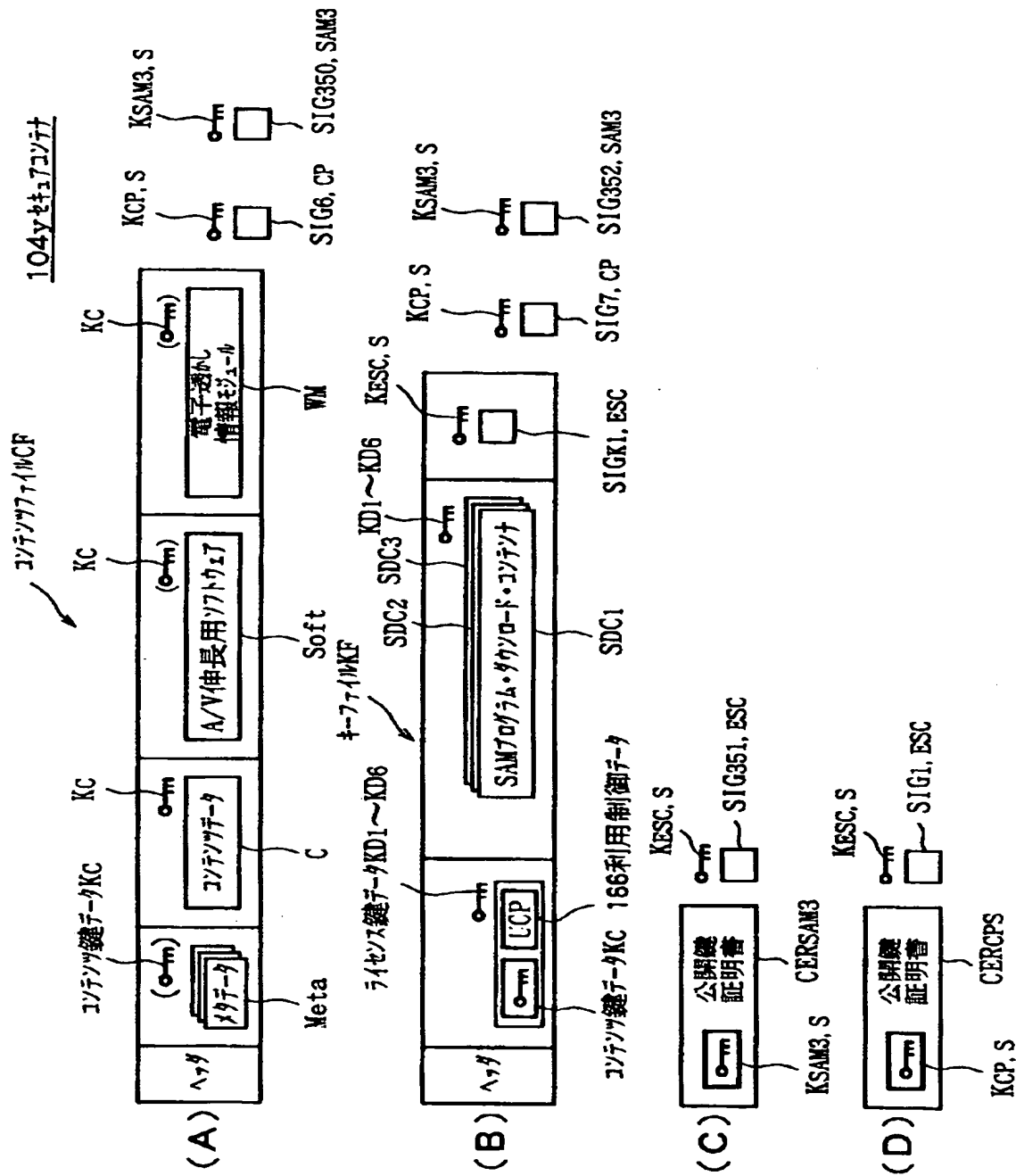
【図 5 2】



【圖 5 3】

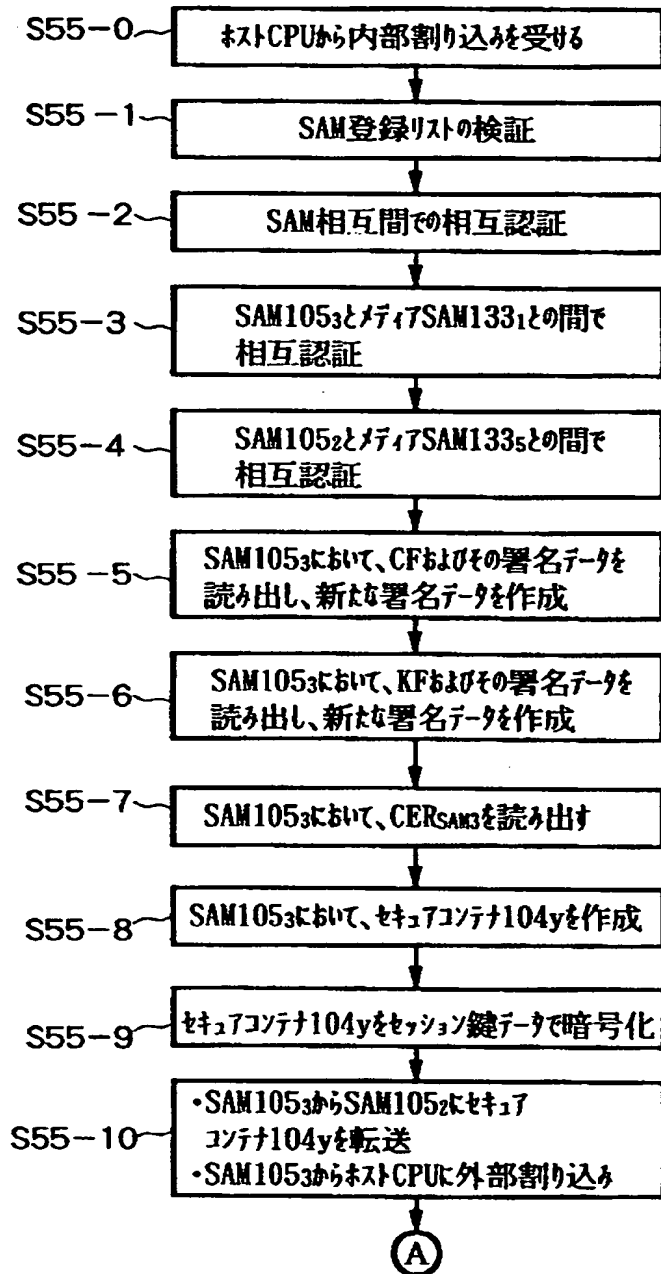


【図 5 4】

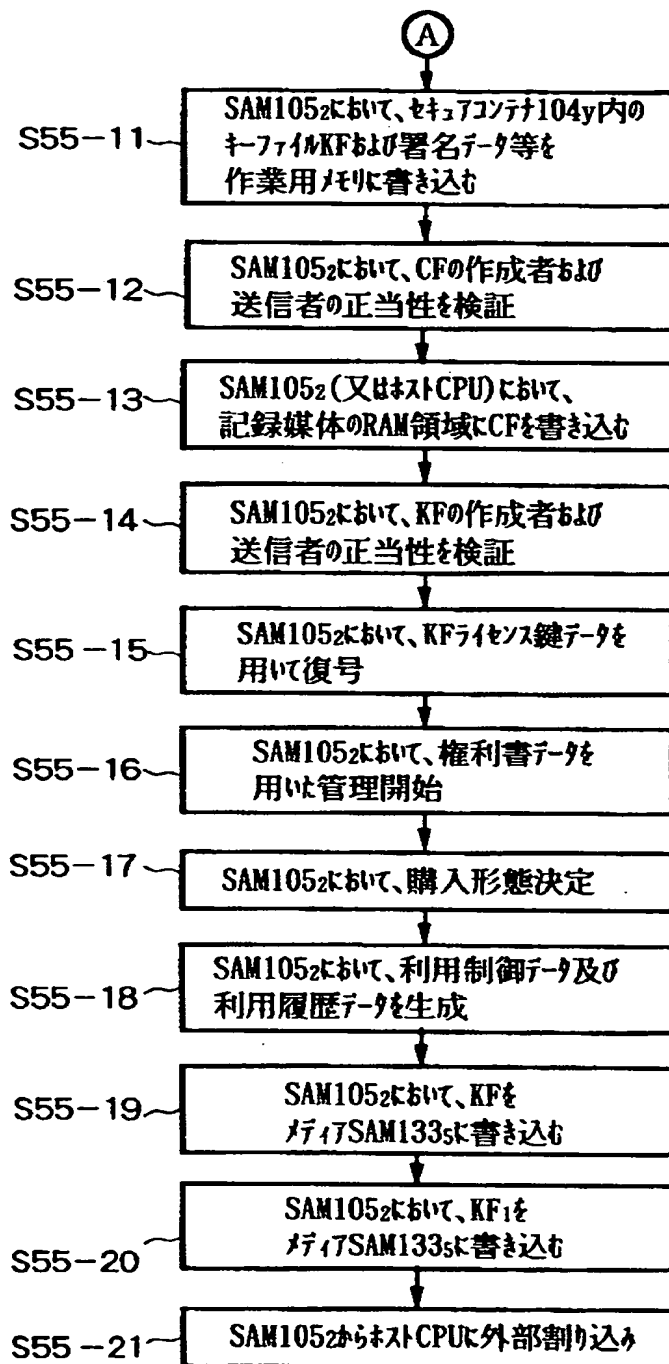


【図 5 5】

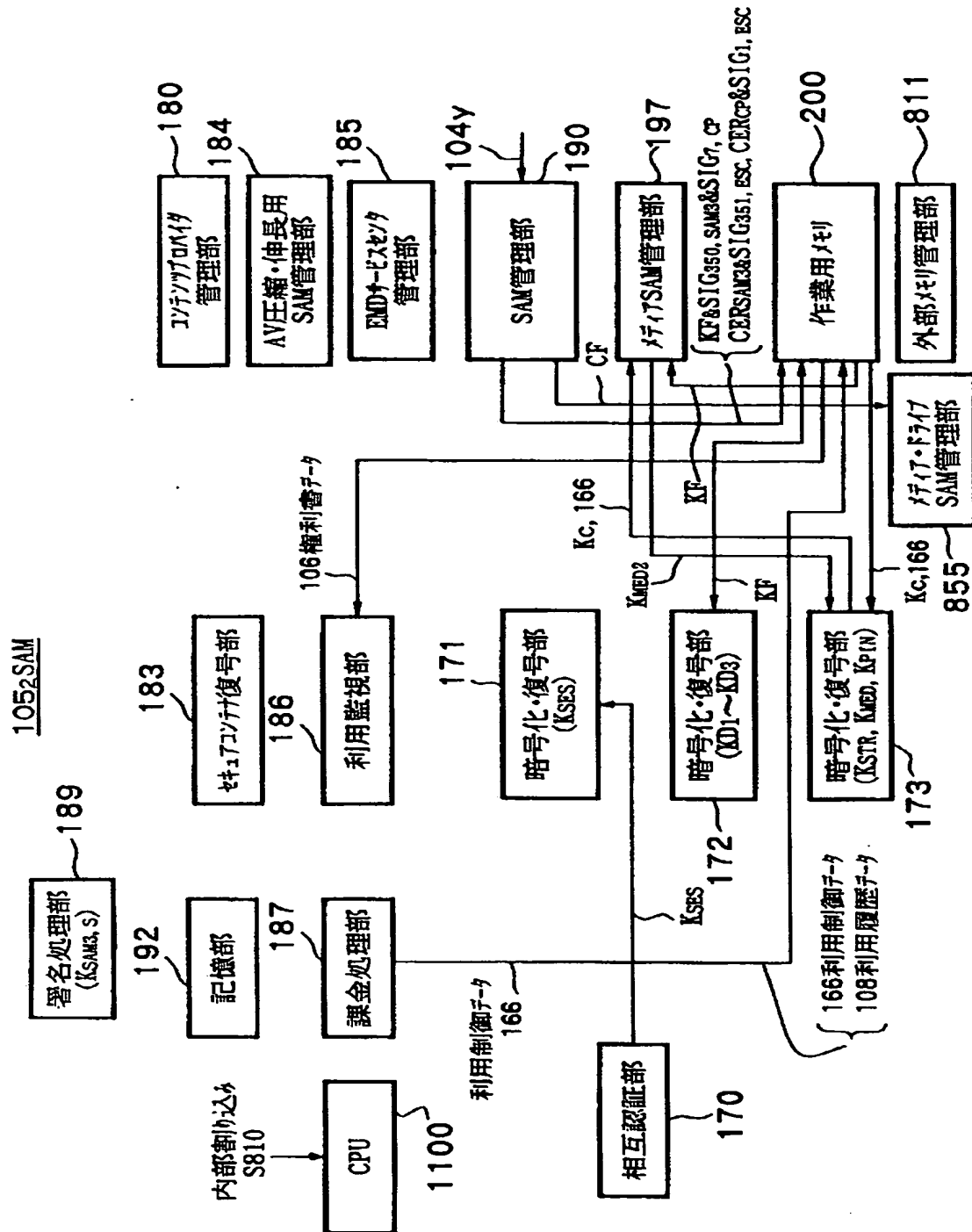
ROM型の記録媒体のコンテンツデータを転送した後転送先で
購入形態を決定してRAM型の記録媒体に書き込む場合の処理



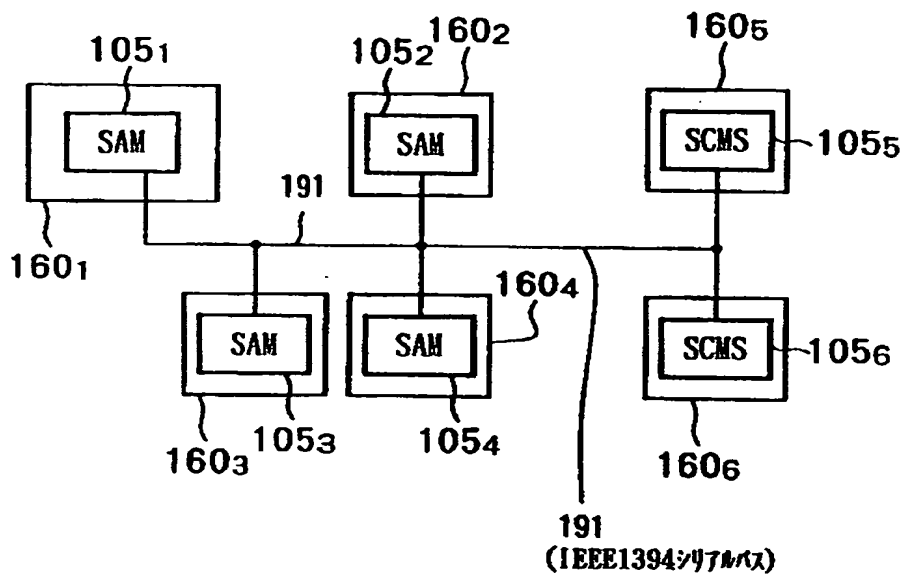
【図 5 6】



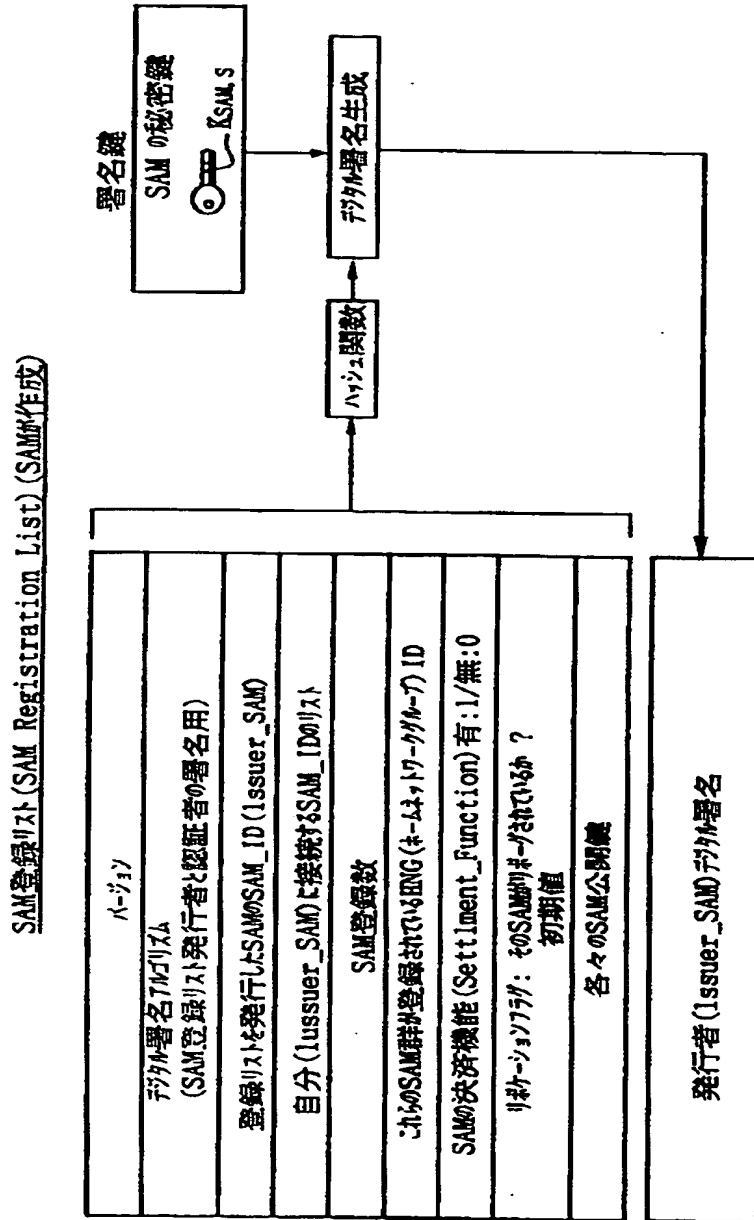
【図 5 7】



【図 5 8】



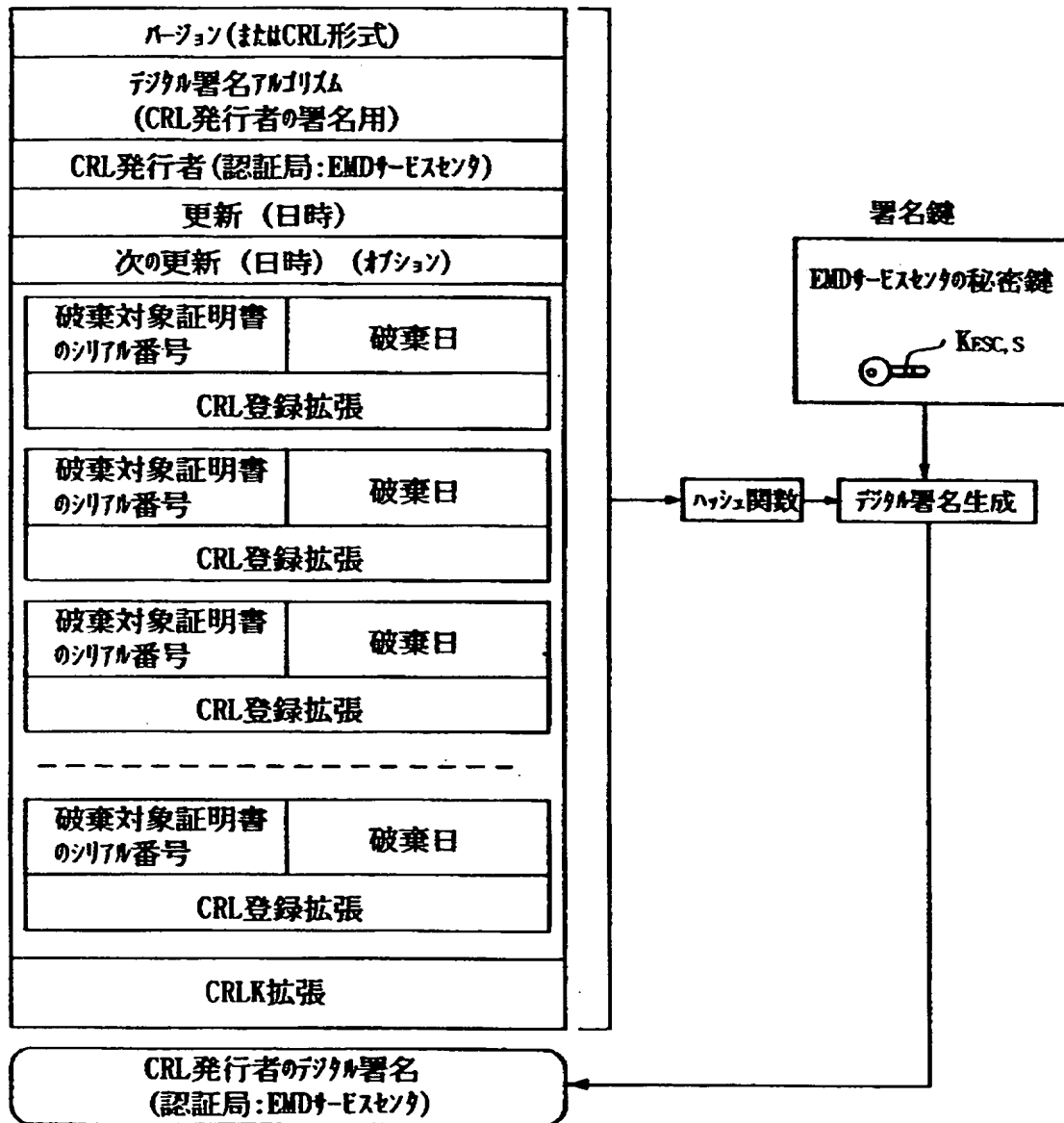
【図 5 9】



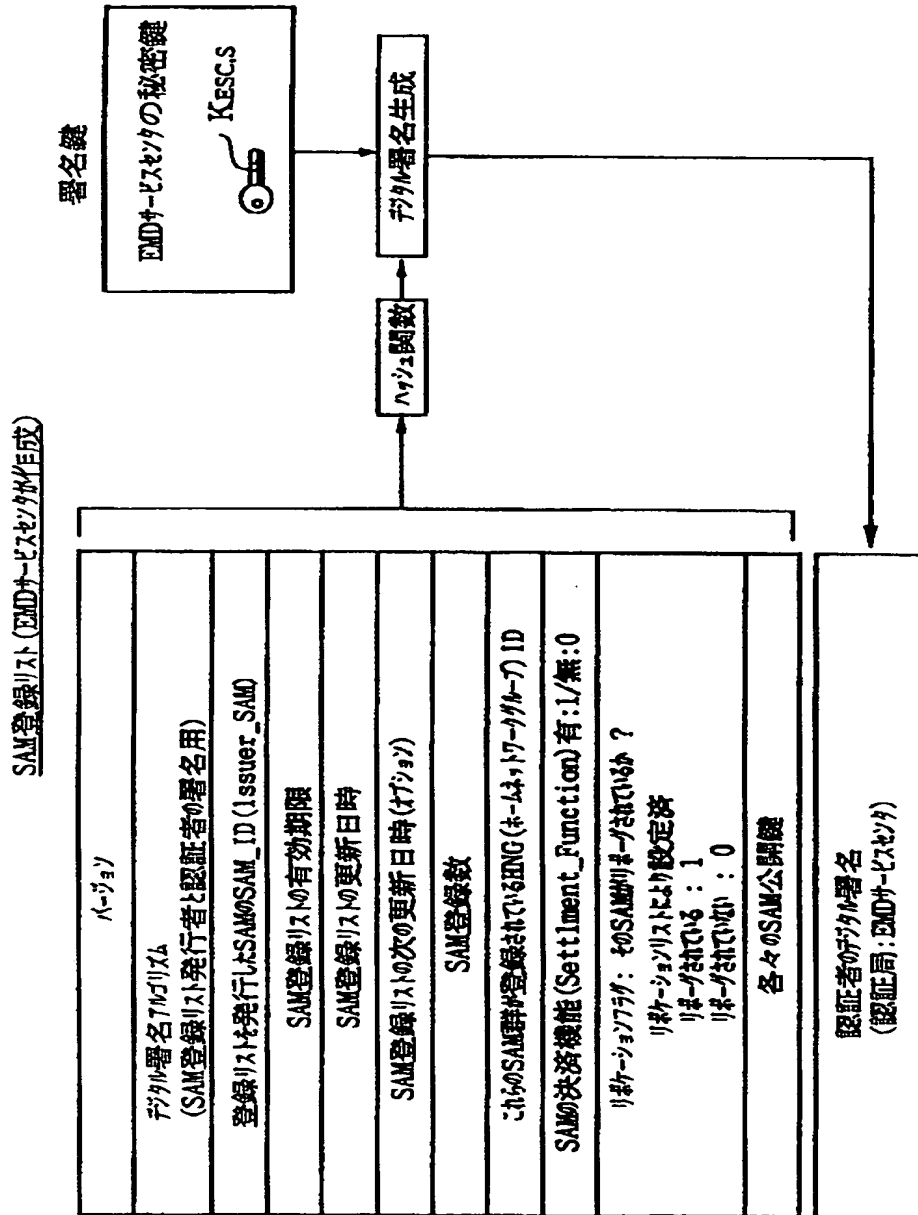
【図 60】

公開鍵証明書破棄リスト (CRL:Certificate Revocation List)

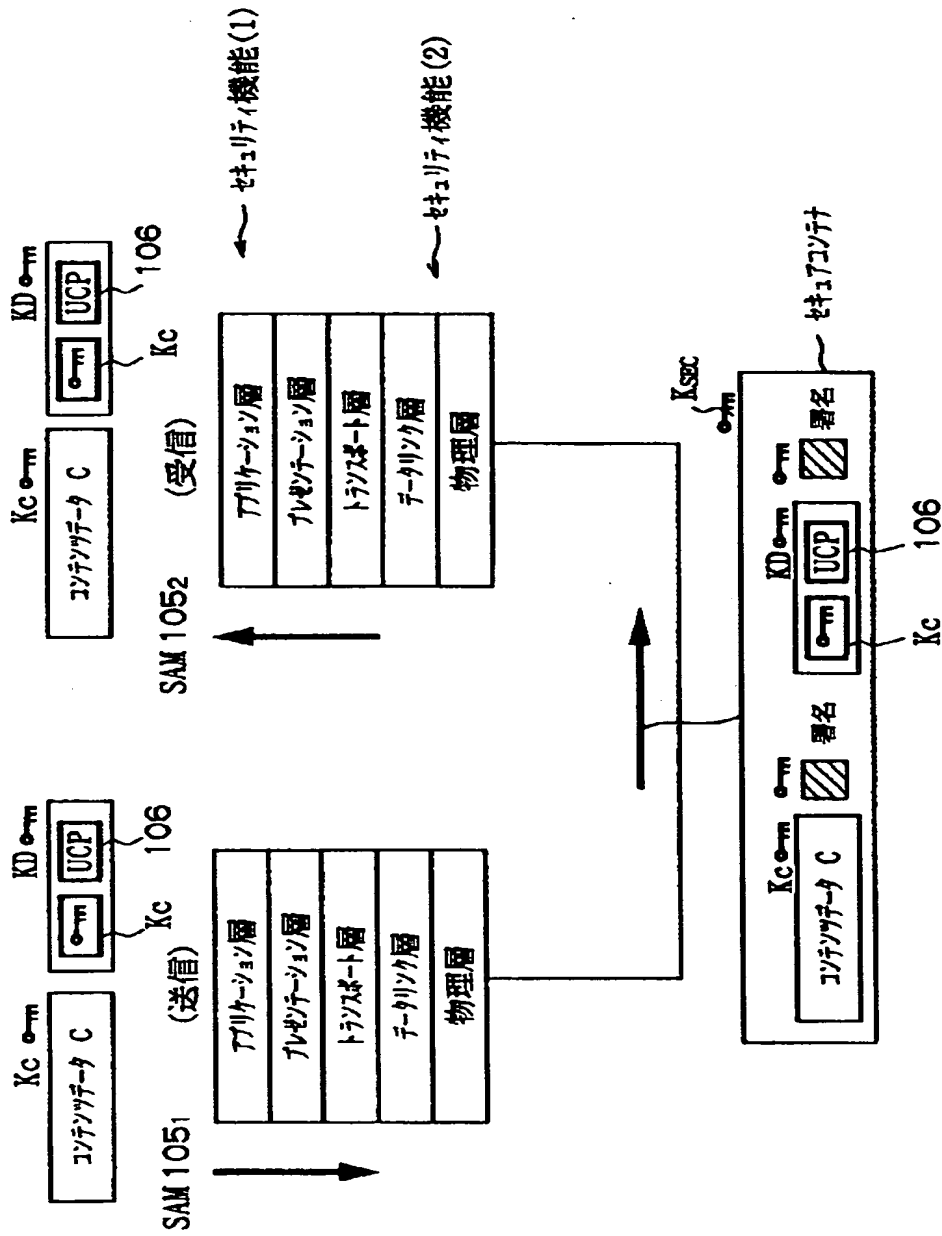
X.509CRL形式



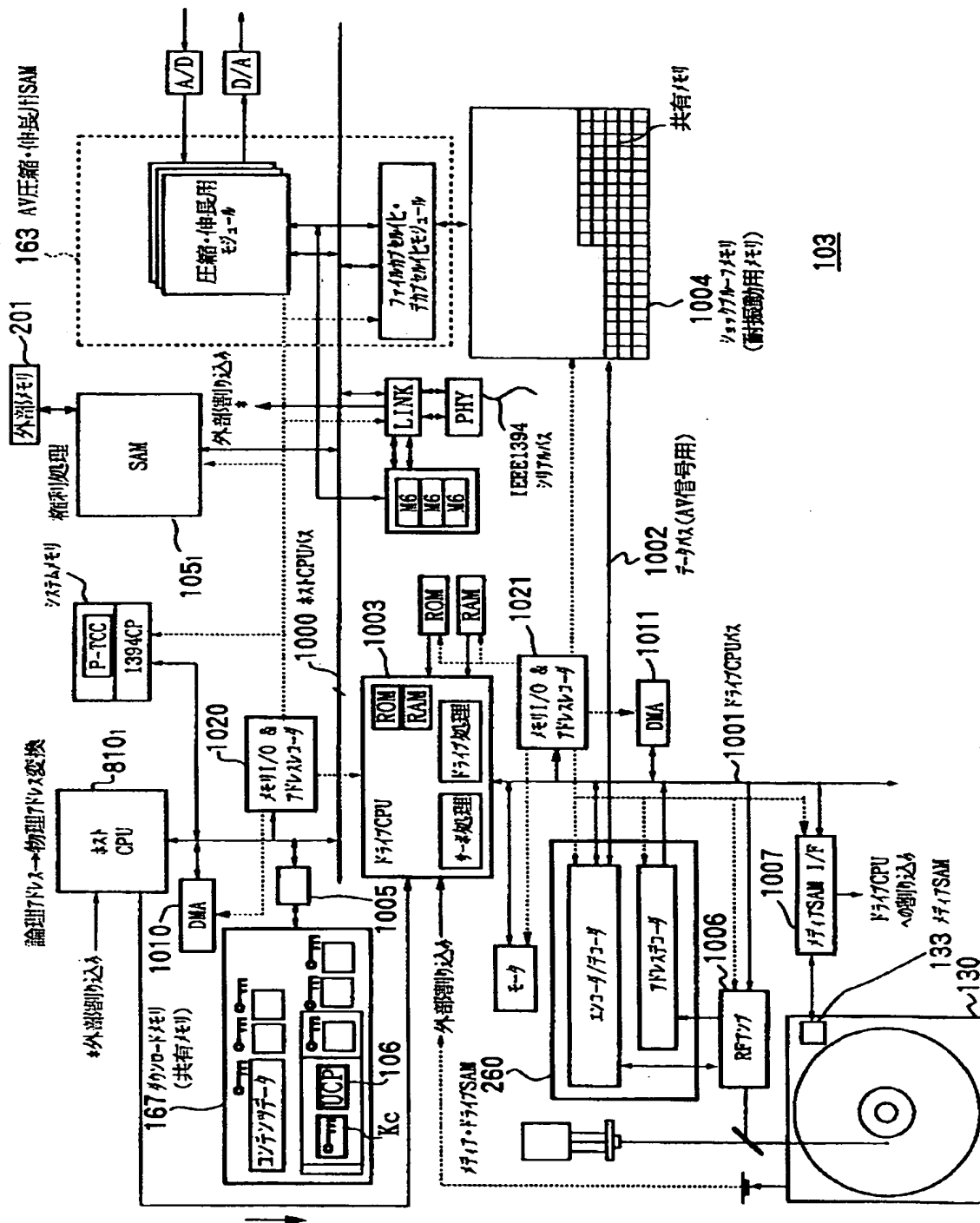
【図 6 1】



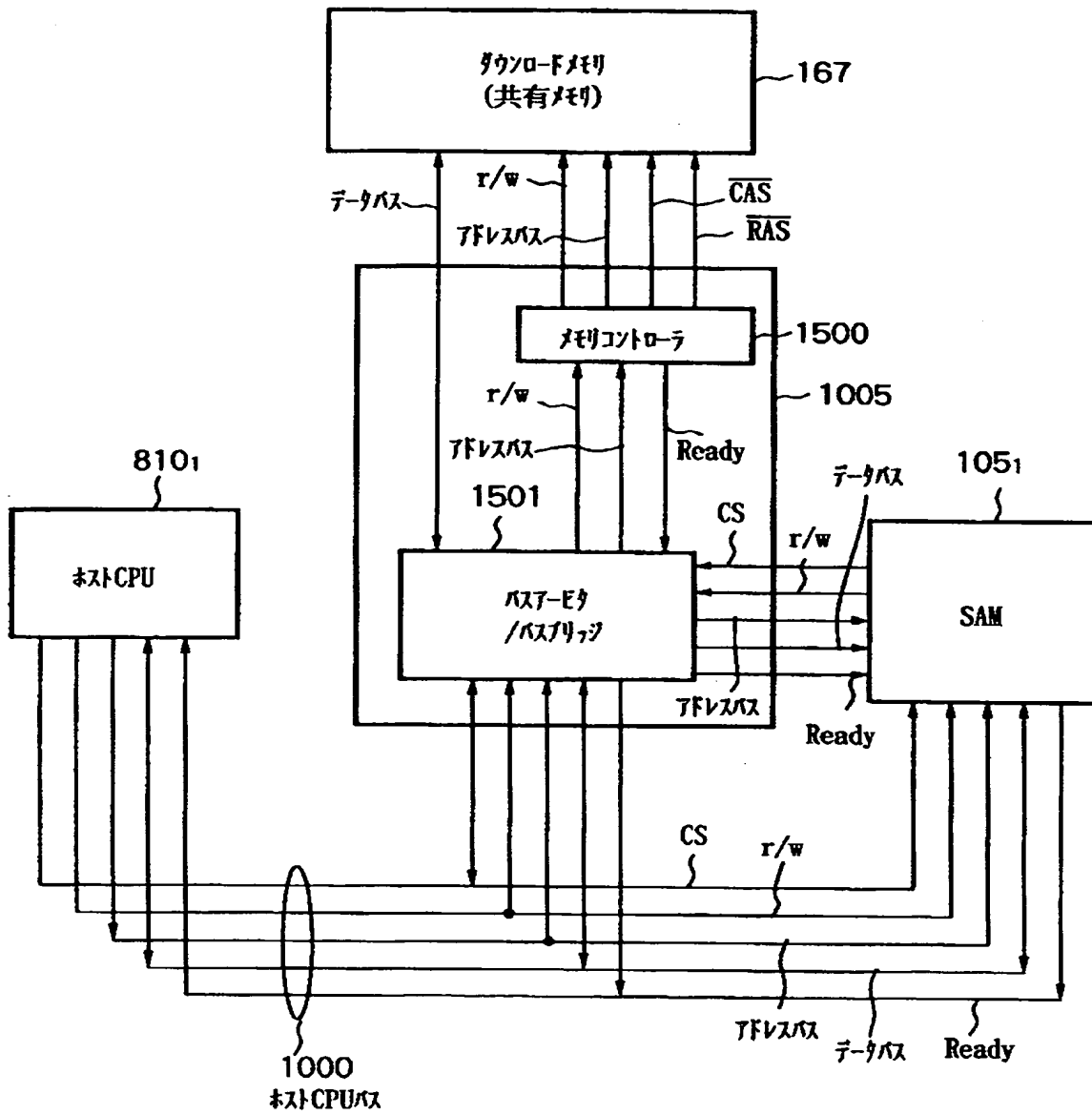
【図 6 2】



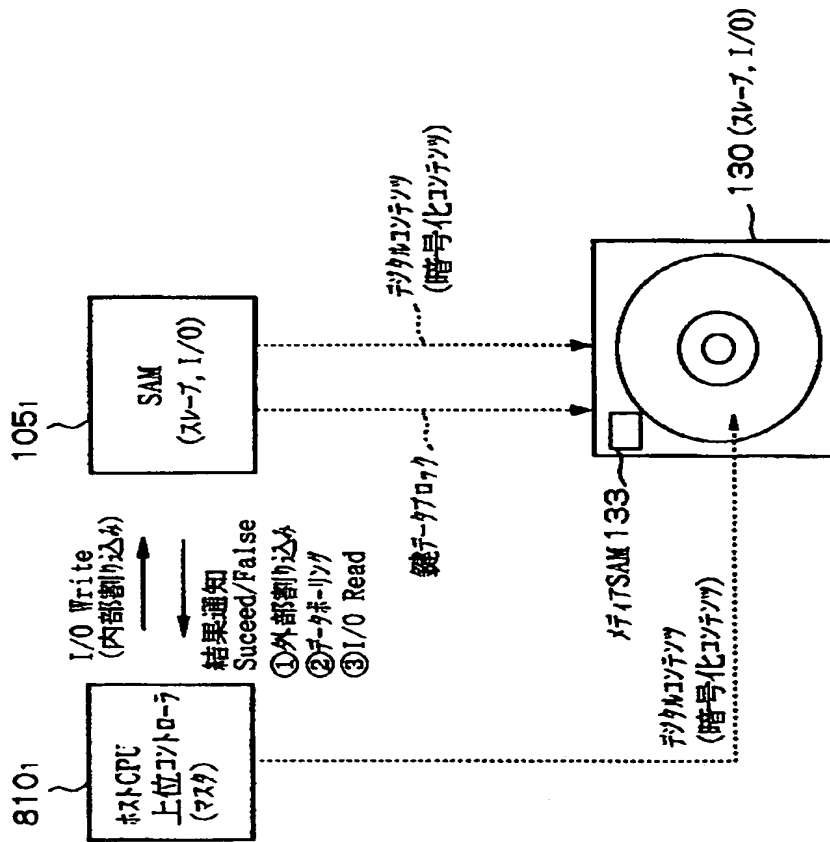
【図 6 3】



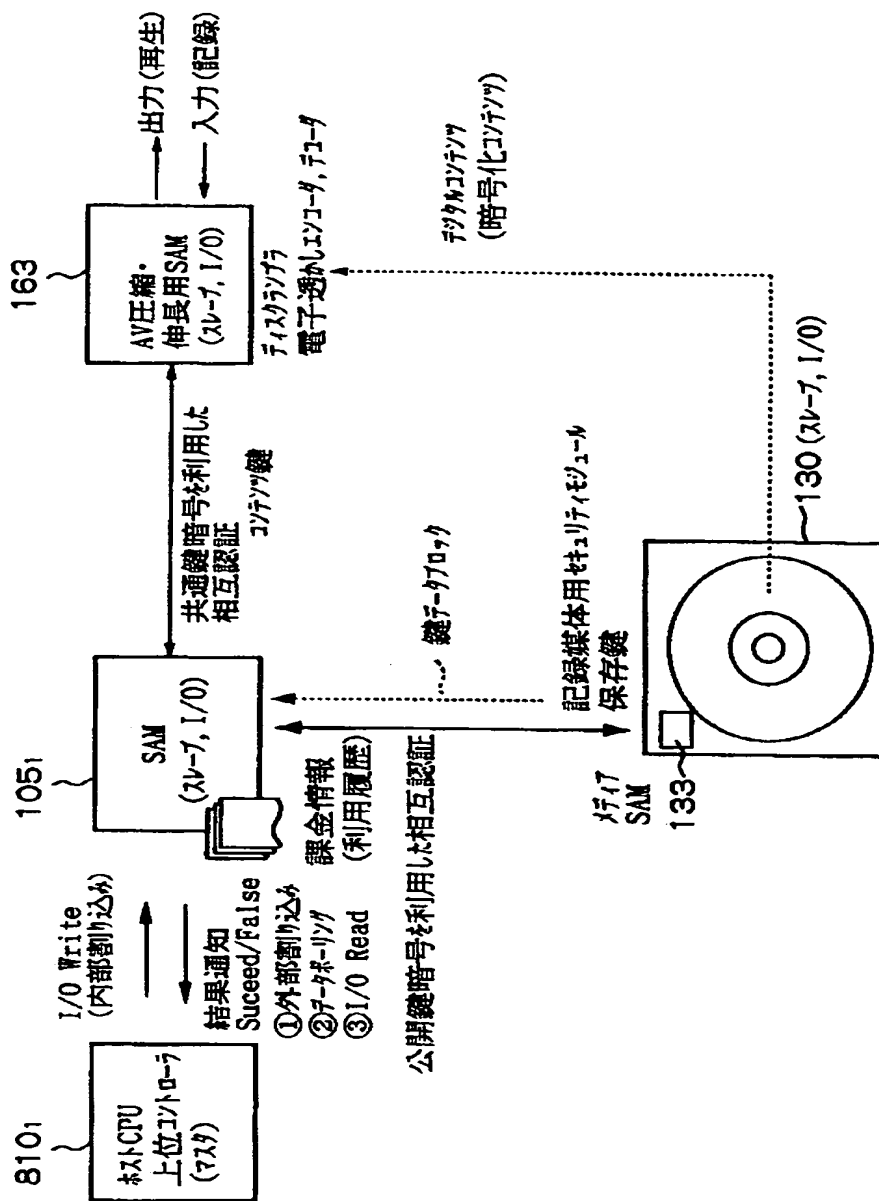
【図 6 4】



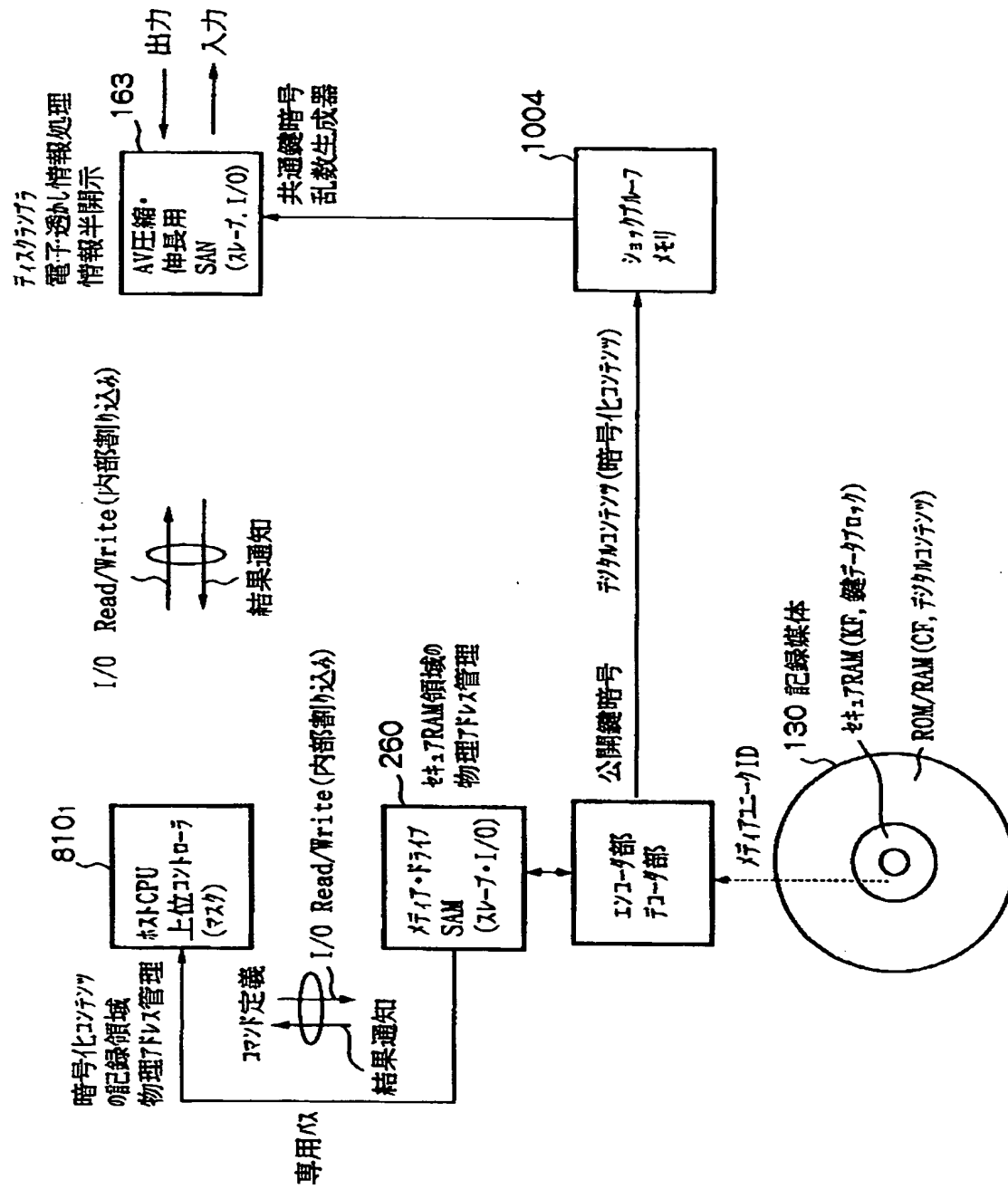
【図 6 5】



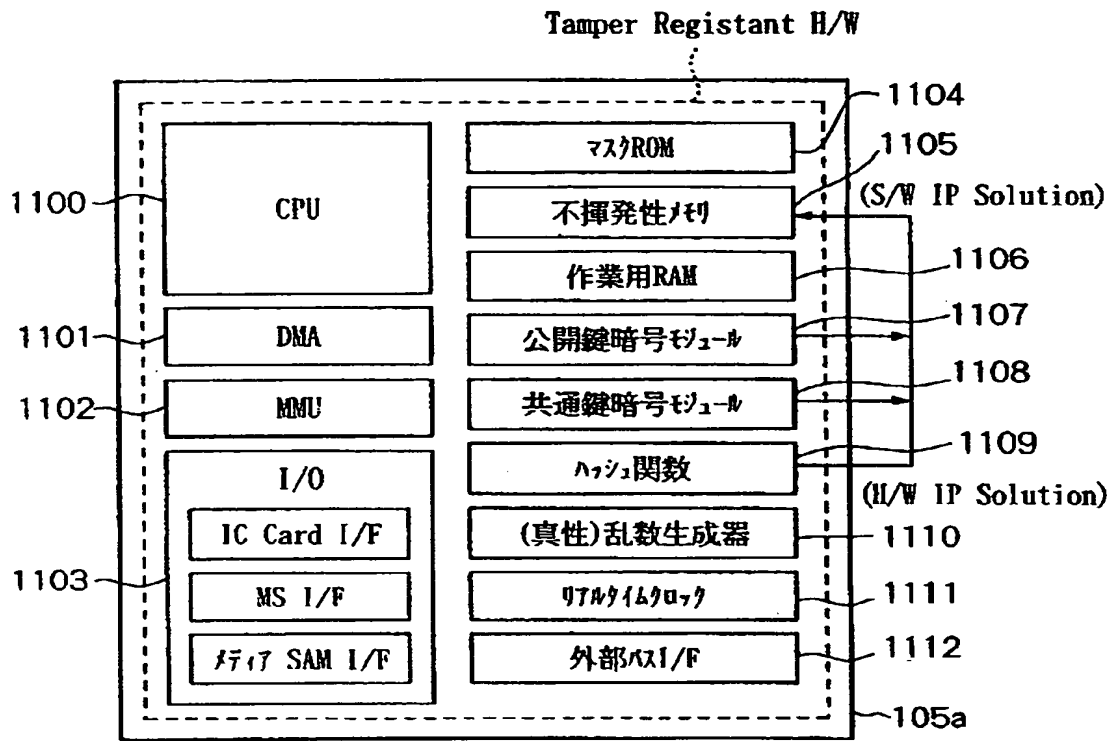
【図 6 6】



【图 6 7】

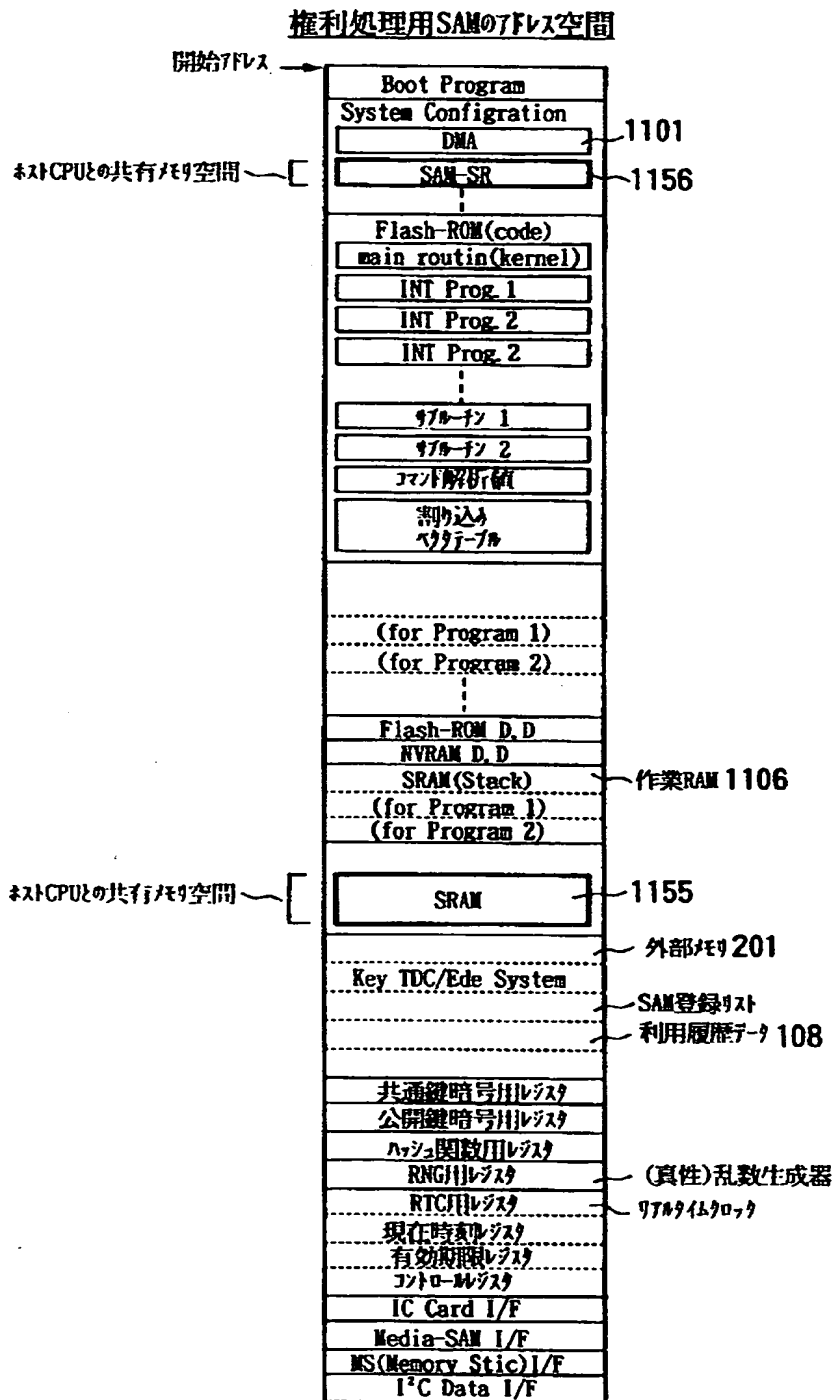


【図 6 8】

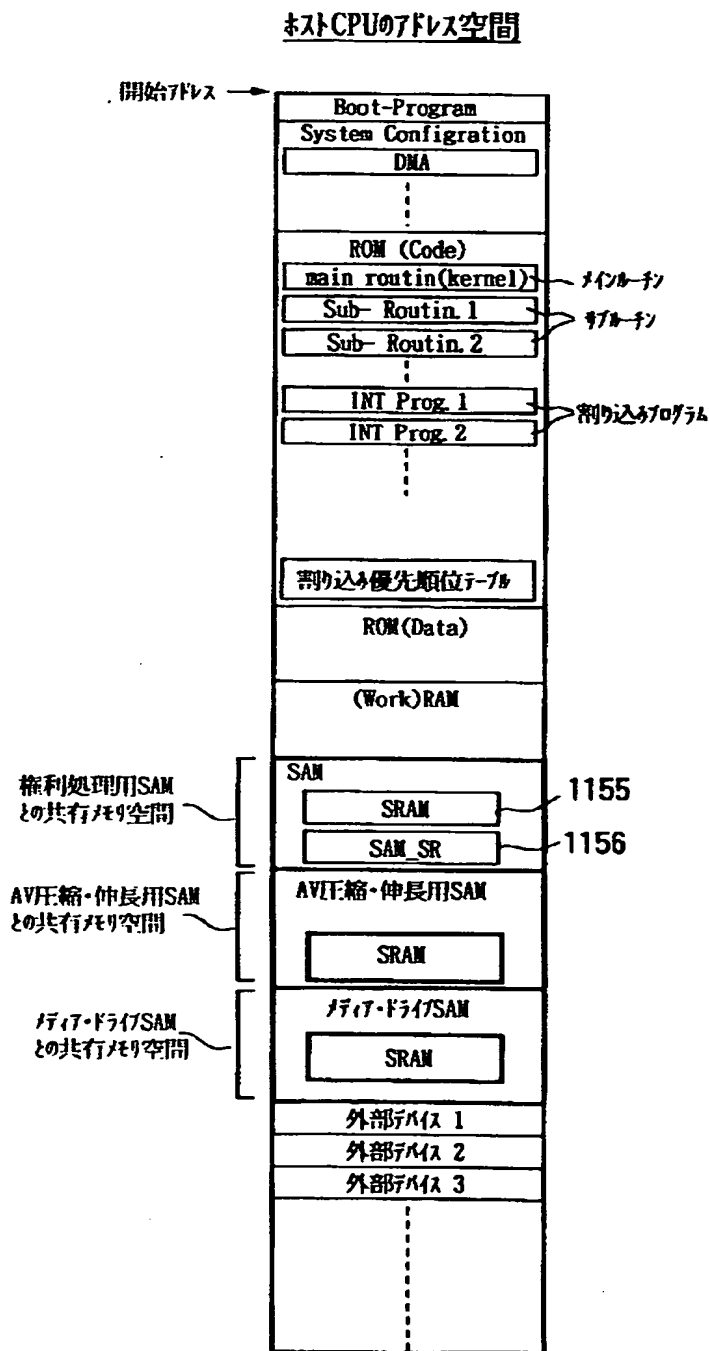


権利処理用のSAM105a

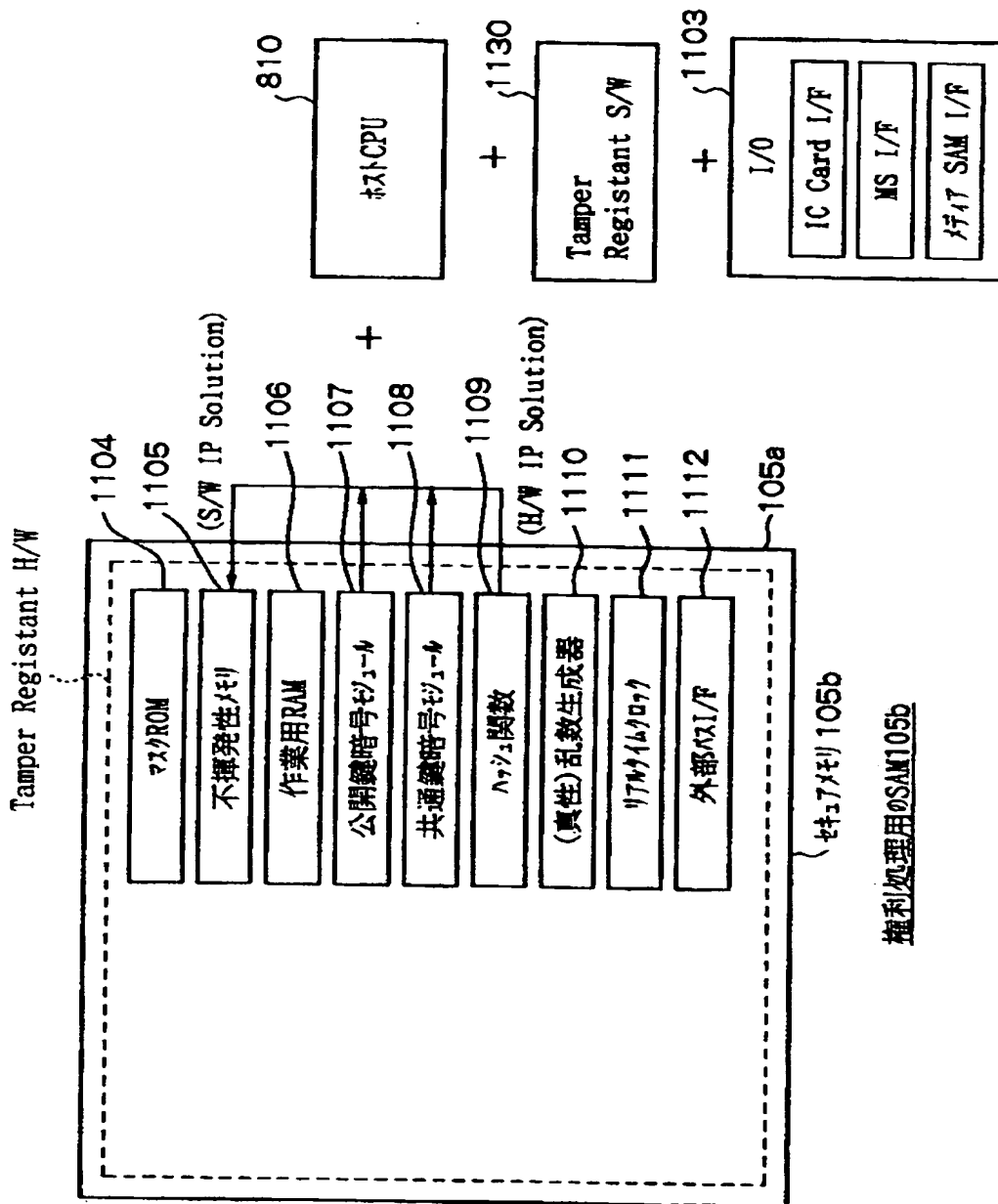
【図 7 0】



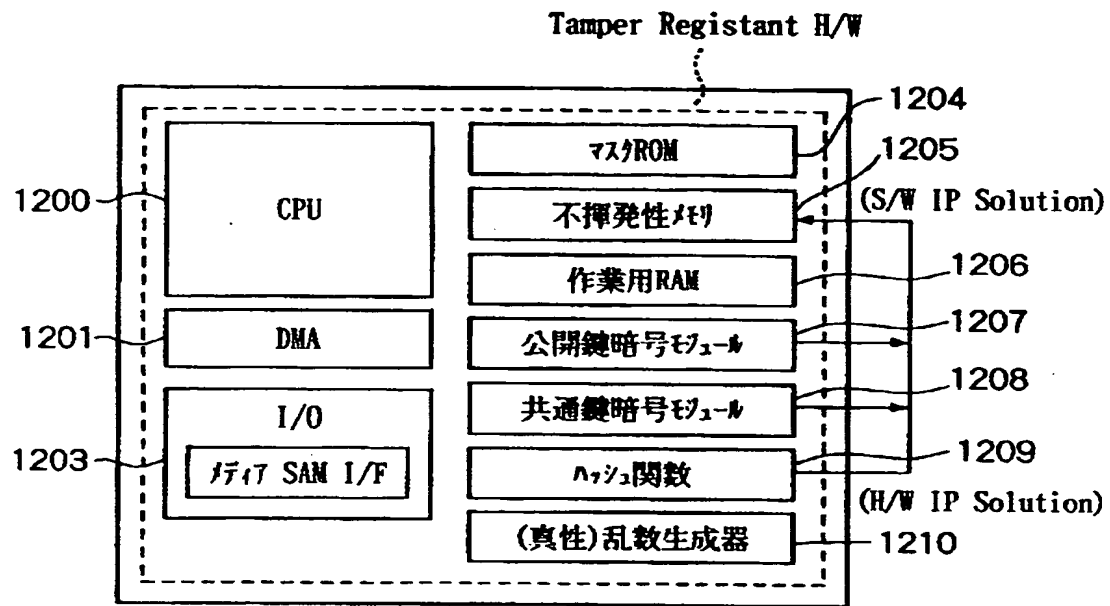
【図 7 1】



【図 7 2】



【図 7 3】



【図 7 4】

メディアSAM ID	
記録用鍵K _{STR} (メディア鍵K _{MED})	
第3信頼機関 (EMDサービスセンタ) の公開鍵	
ルートCAの公開鍵	
メディアSAM公開鍵証明書 (X. 509)	
メディアSAM公開鍵・秘密鍵	
Revocation List (更新値)	
権利処理 (利益配分) 用データ	
利益分配しない関連エンティティのID	
メディアタイプ	
<ul style="list-style-type: none"> ・メディアの種別情報 ・ROM/RAM 	
キーファイルKFの物理アドレス情報 (レジスタ空間)	検証値
検証値 (MAC)	
コンテンツナンバー #1 のKF	検証値 (MAC)
コンテンツナンバー #2 のKF	
コンテンツナンバー #3 のKF	
コンテンツナンバー #4 のKF	
コンテンツナンバー #5 のKF	
コンテンツナンバー #n のKF	検証値 (MAC)
検証値 (MAC)	

ライセンス鍵KDによる
暗号文

ROM型の記録媒体のメディアSAMの記憶データ (出荷時)

【図 7 5】

メディアSAM ID	
記録用鍵KSTR(メディア鍵K _{MED})	
User ID	
パスワード	
個人嗜好情報	
個人決済情報(クレジットカード番号)	
電子マネー	
第3信頼機関(EMDサービスセンタ)の公開鍵	
ルートCAの公開鍵	
メディアSAM公開鍵証明書(X.509)	
メディアSAM公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分配しだい関連エンティティのID	
メディアタイプ	
・メディアの種別情報	
・ROM/RAM	
キーファイルKFの物理アドレス情報 (レジスタ空間)	検証値
検証値(MAC)	
コンテンツナンバー#1のKF/KF ₁	
コンテンツナンバー#2のKF/KF ₁	
コンテンツナンバー#3のKF/KF ₁	
コンテンツナンバー#4のKF/KF ₁	
コンテンツナンバー#5のKF/KF ₁	
	検証値(MAC)
コンテンツナンバー#nのKF/KF ₁	
検証値(MAC)	

ライセンス鍵KDによる
暗号文

ROM型の記録媒体のメディアSAMの記憶データ(登録及び購入処理後)

【図 7 6】

マイSAM ID
記録用鍵KSTR(マイ鍵KME)
第3信頼機関(EMDサービスセンター)の公開鍵
ルートCAの公開鍵
マイSAM公開鍵証明書(X. 509)
マイSAM公開鍵・秘密鍵
Revocation List(更新値)
権利処理(利益配分)用データ
利益分配しない関連エンティティのID
マイタイプ
・マイの種別情報
・ROM/RAM

RAMの記録媒体のマイSAMの記憶データ(出荷時)

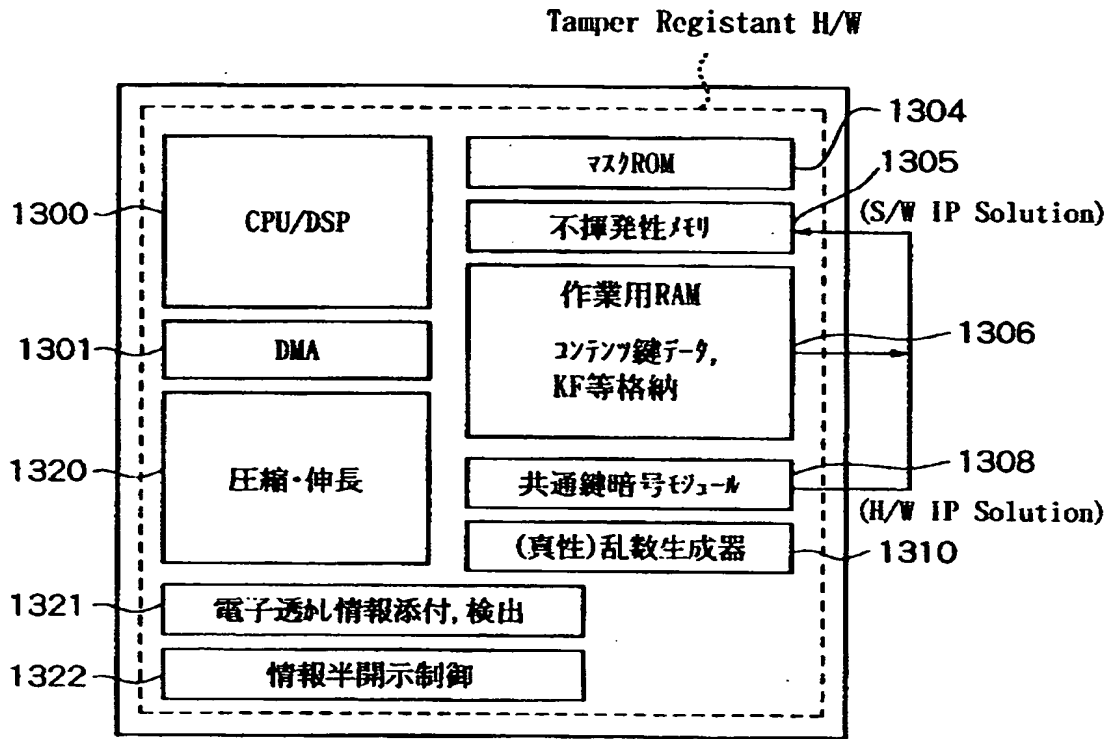
【図 7 7】

マイSAM ID	
記録用鍵K _{STR} (マイ鍵K _{MD})	
User ID	
パスワード	
個人嗜好情報	
個人決済情報(クレジットカード番号)	
電子マネー	
第3信頼機関(EMDサービスセンター)の公開鍵	
ルートCAの公開鍵	
マイSAM公開鍵証明書(X.509)	
マイSAM公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分配したい関連エンティティのID	
マイタイプ	
・マイの種別情報	
・ROM/RAM	
キーファイルKFの物理アドレス情報 (レジスタ空間)	検証値
検証値(MAC)	
コンテンツ番号#1のKF/KF ₁	
コンテンツ番号#2のKF/KF ₁	
コンテンツ番号#3のKF/KF ₁	
コンテンツ番号#4のKF/KF ₁	
コンテンツ番号#5のKF/KF ₁	検証値 (MAC)
コンテンツ番号#nのKF/KF ₁	
検証値(MAC)	

記録用鍵K_{STR}による
暗号文

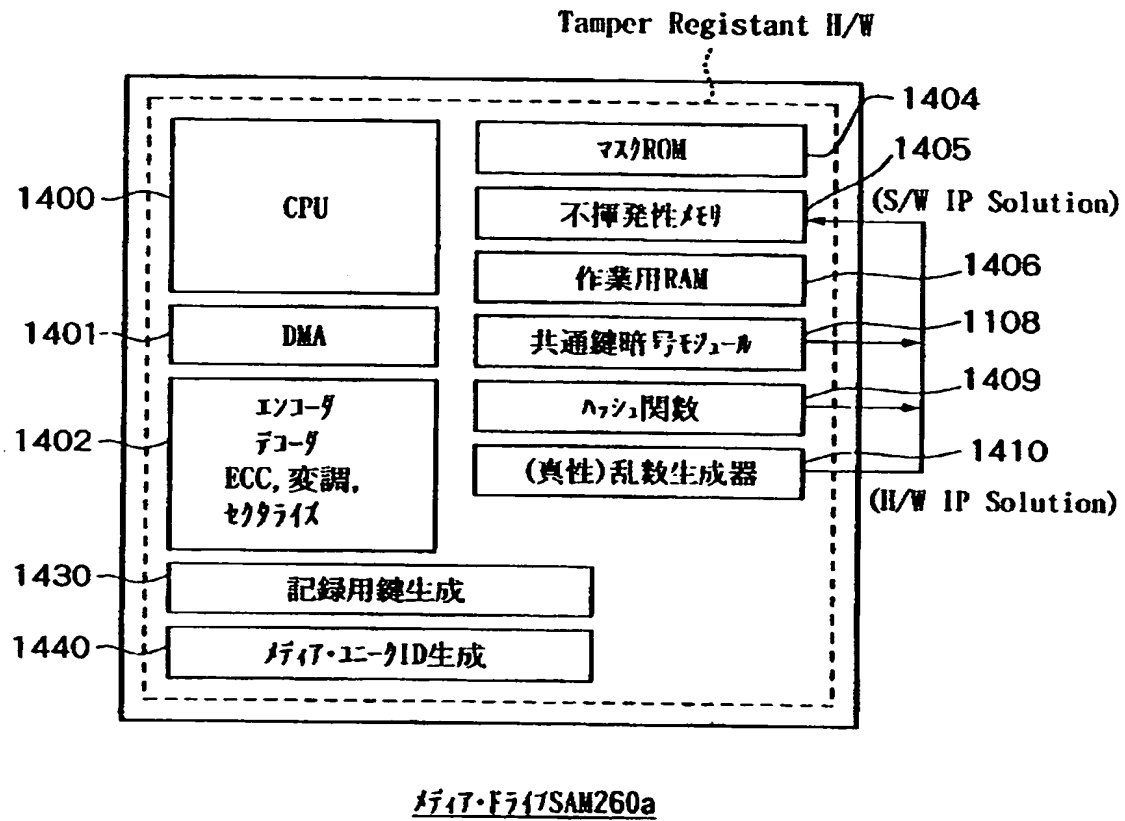
RAMの記録媒体のマイSAMの記憶データ(登録及び購入処理後)

【図 7 8】

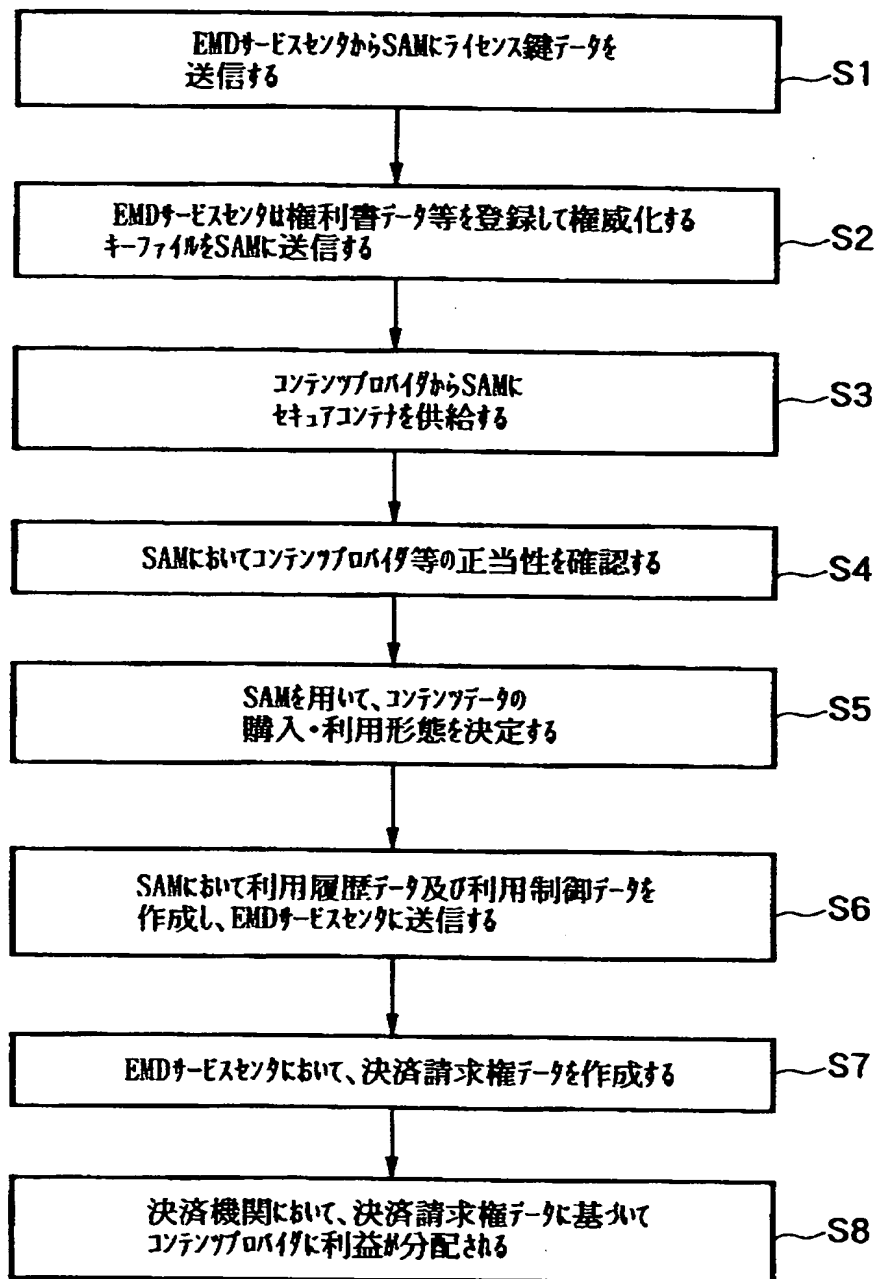


AV圧縮・伸長用SAM163

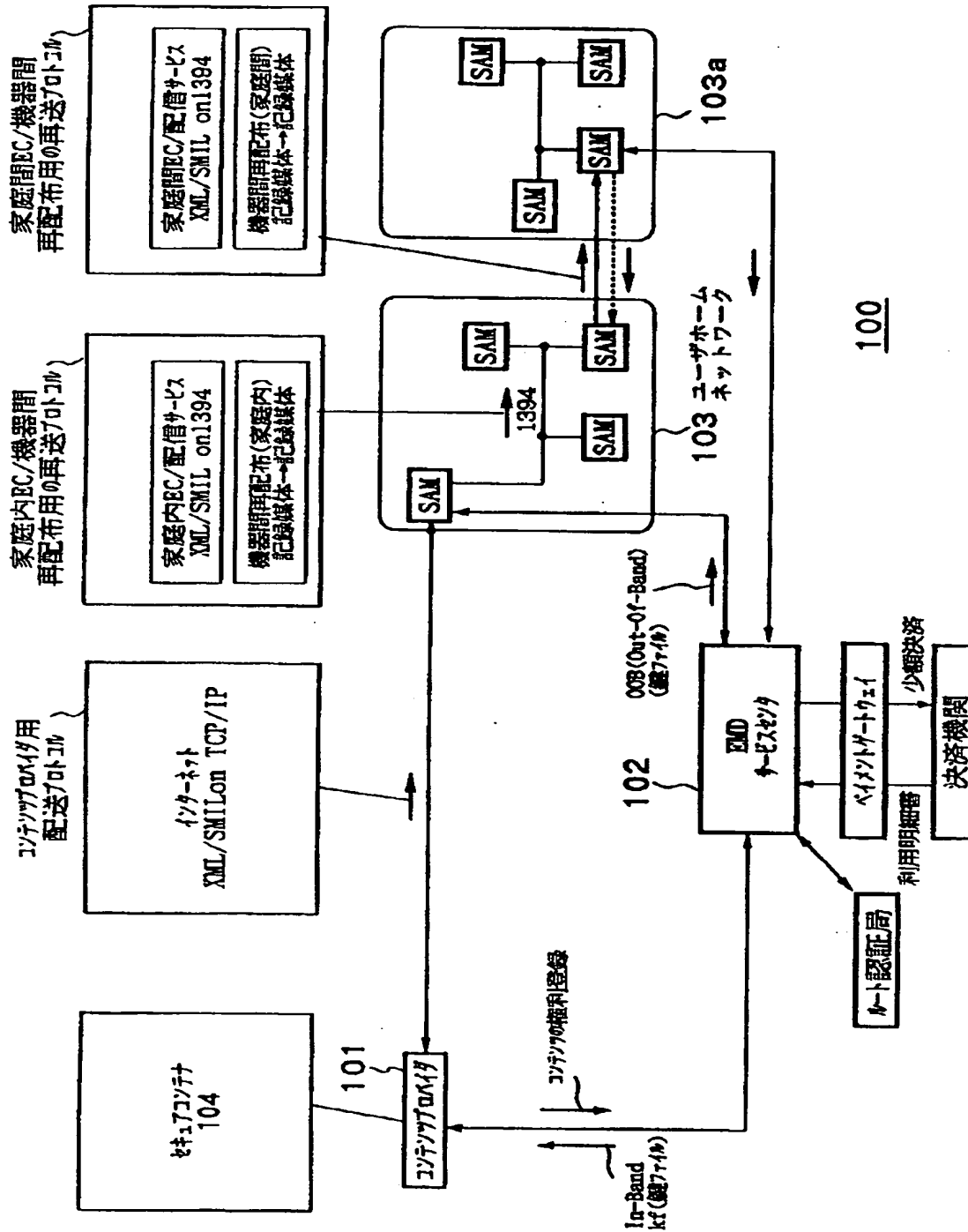
【図 7 9】



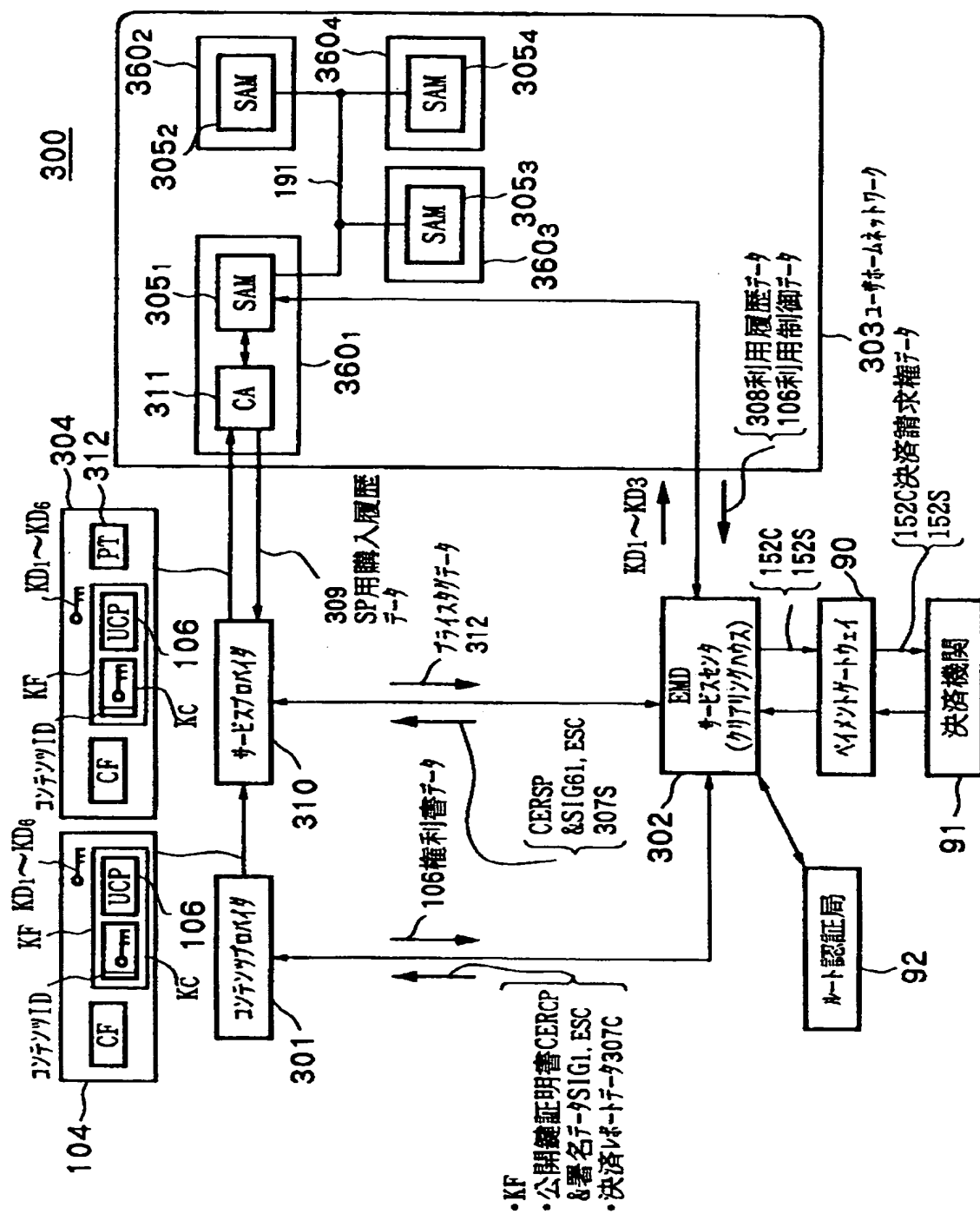
【図 8 0】



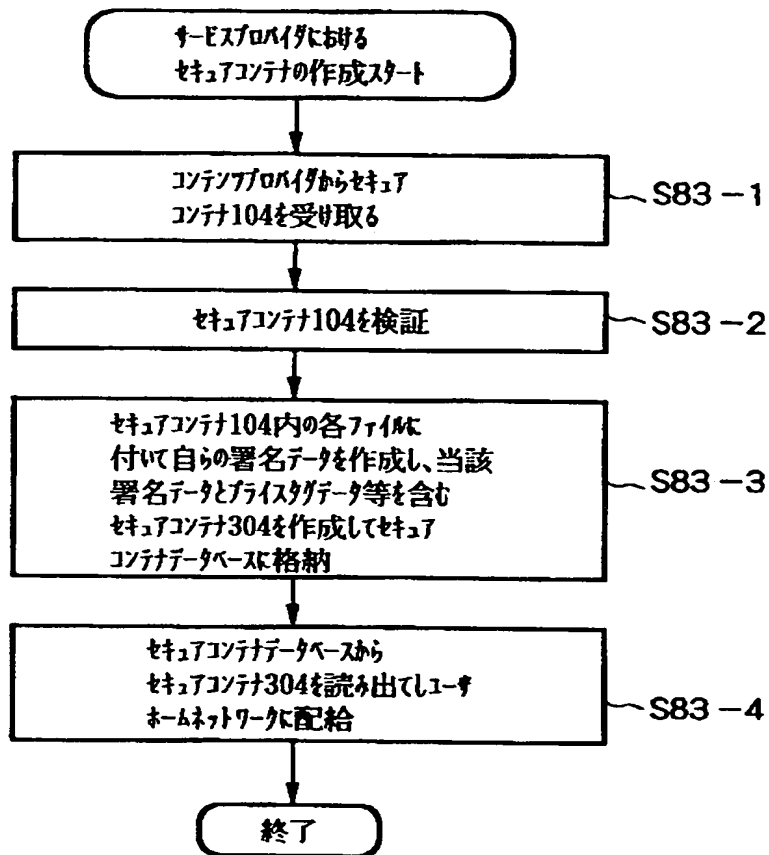
【図 81】



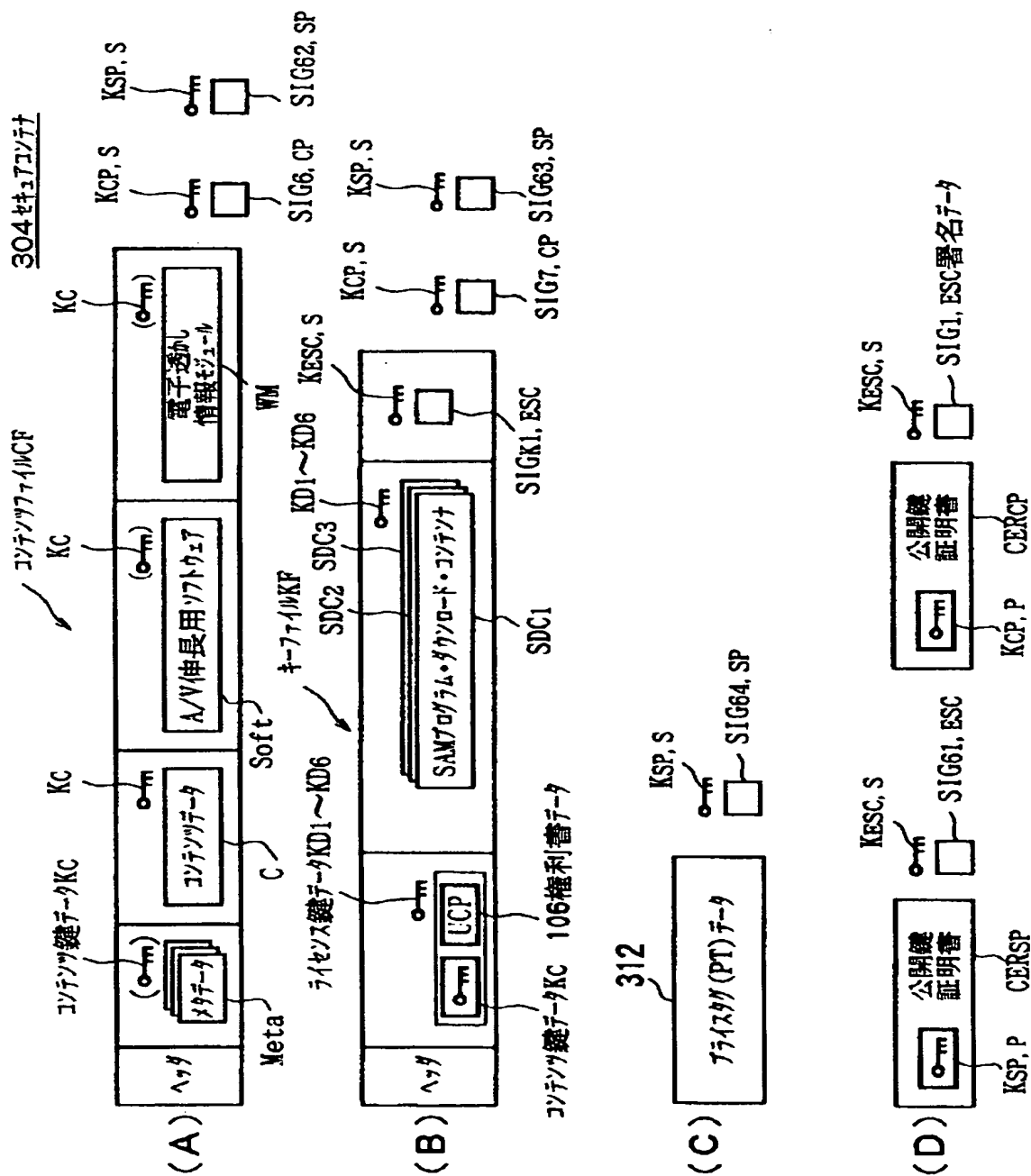
【图 8 2】



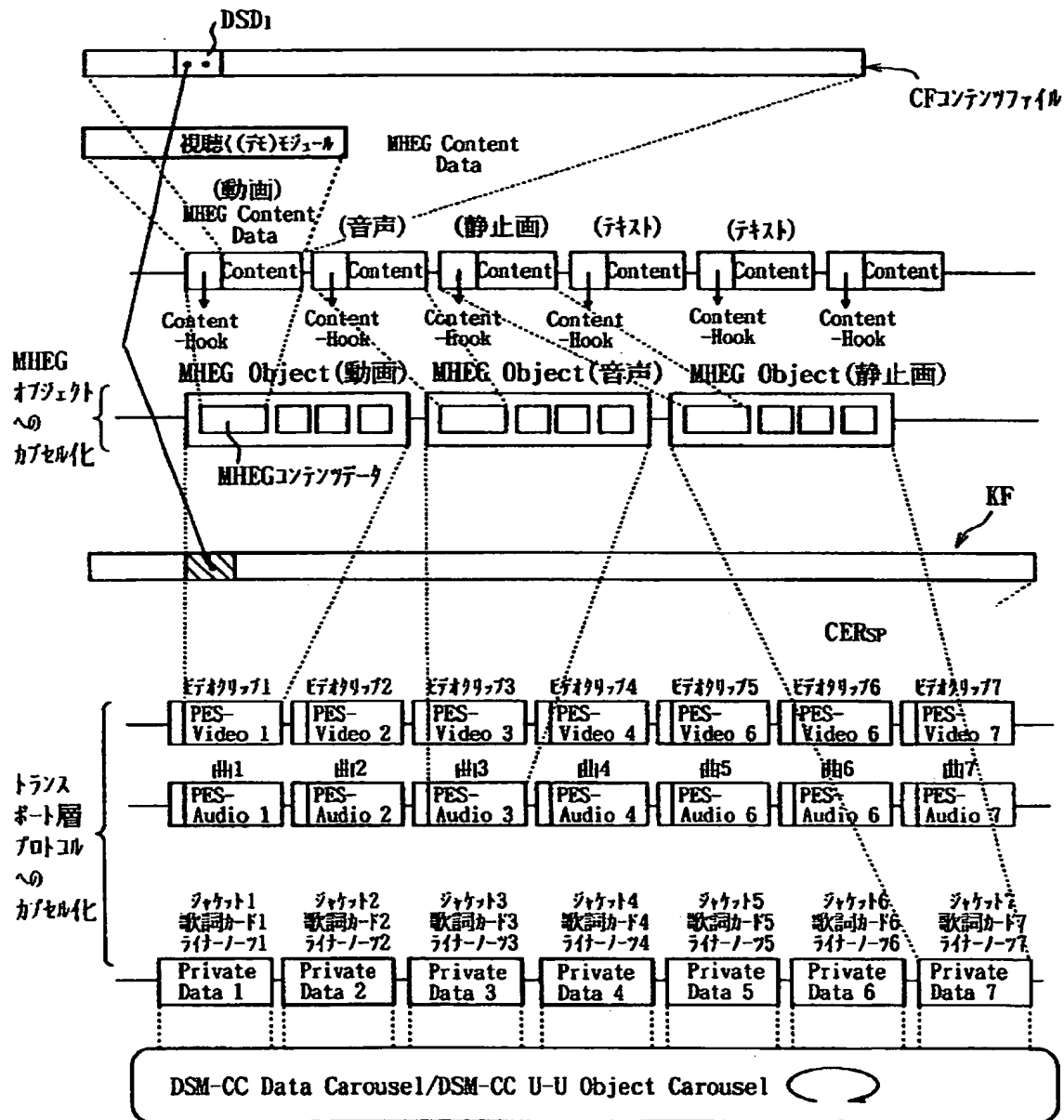
【図 83】



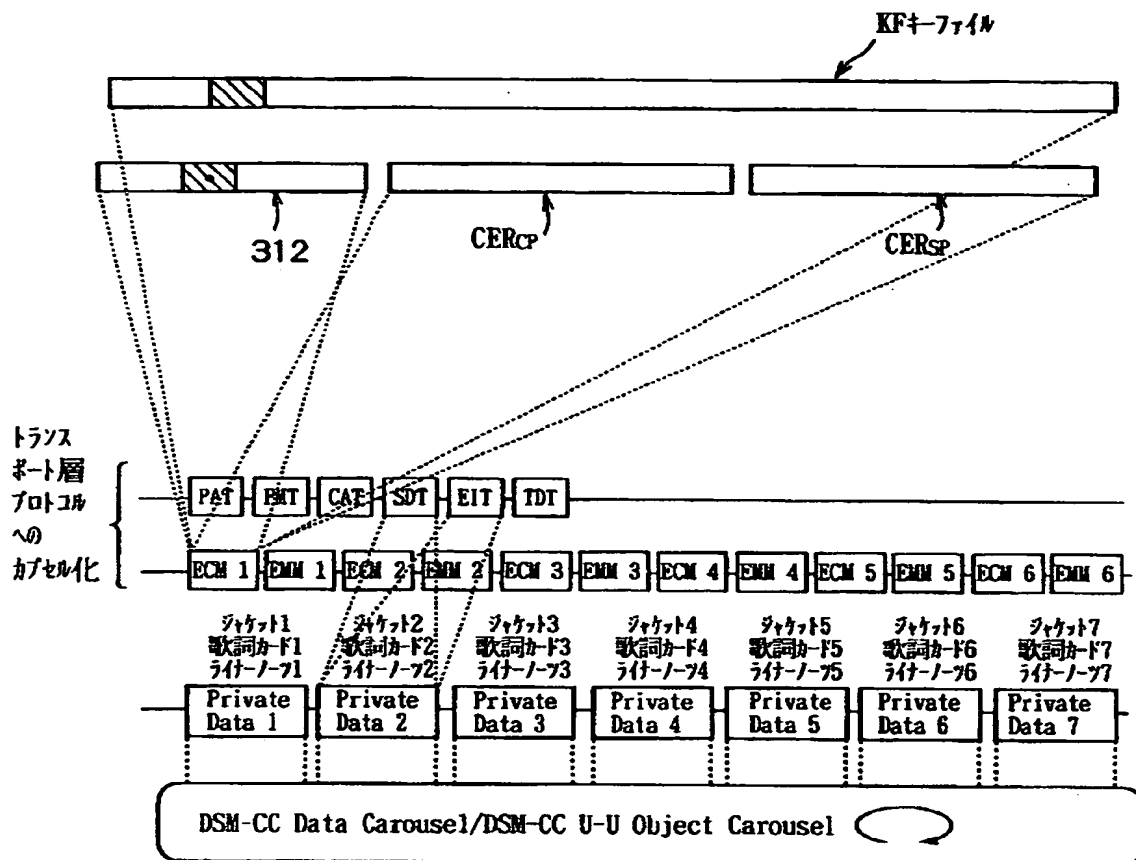
【図 8 4】



【図 8 5】



【図 8 6】



【図 8 7】

EMDサービス302の主な機能

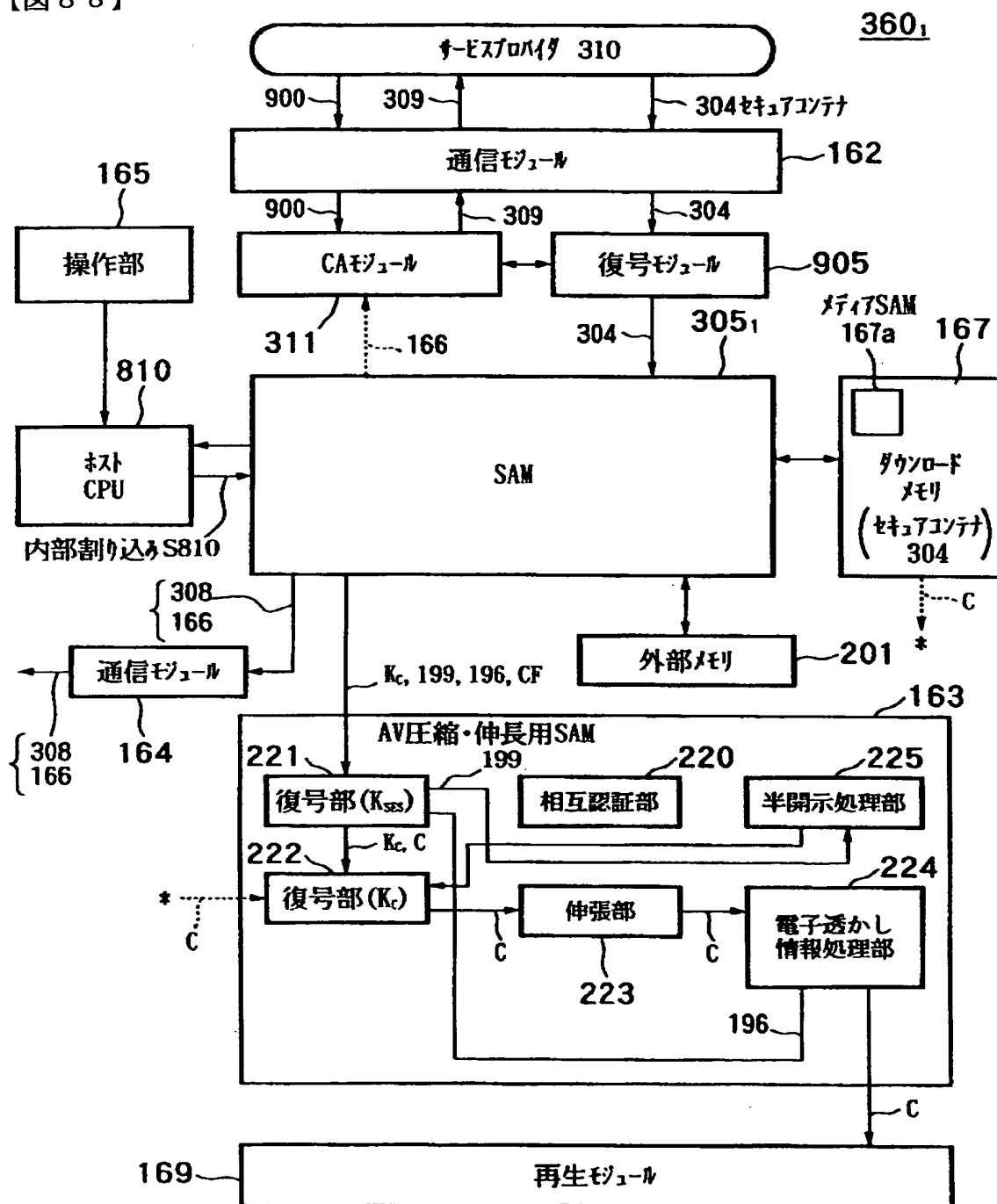
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給

公開鍵証明書データDER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAM4}の発行

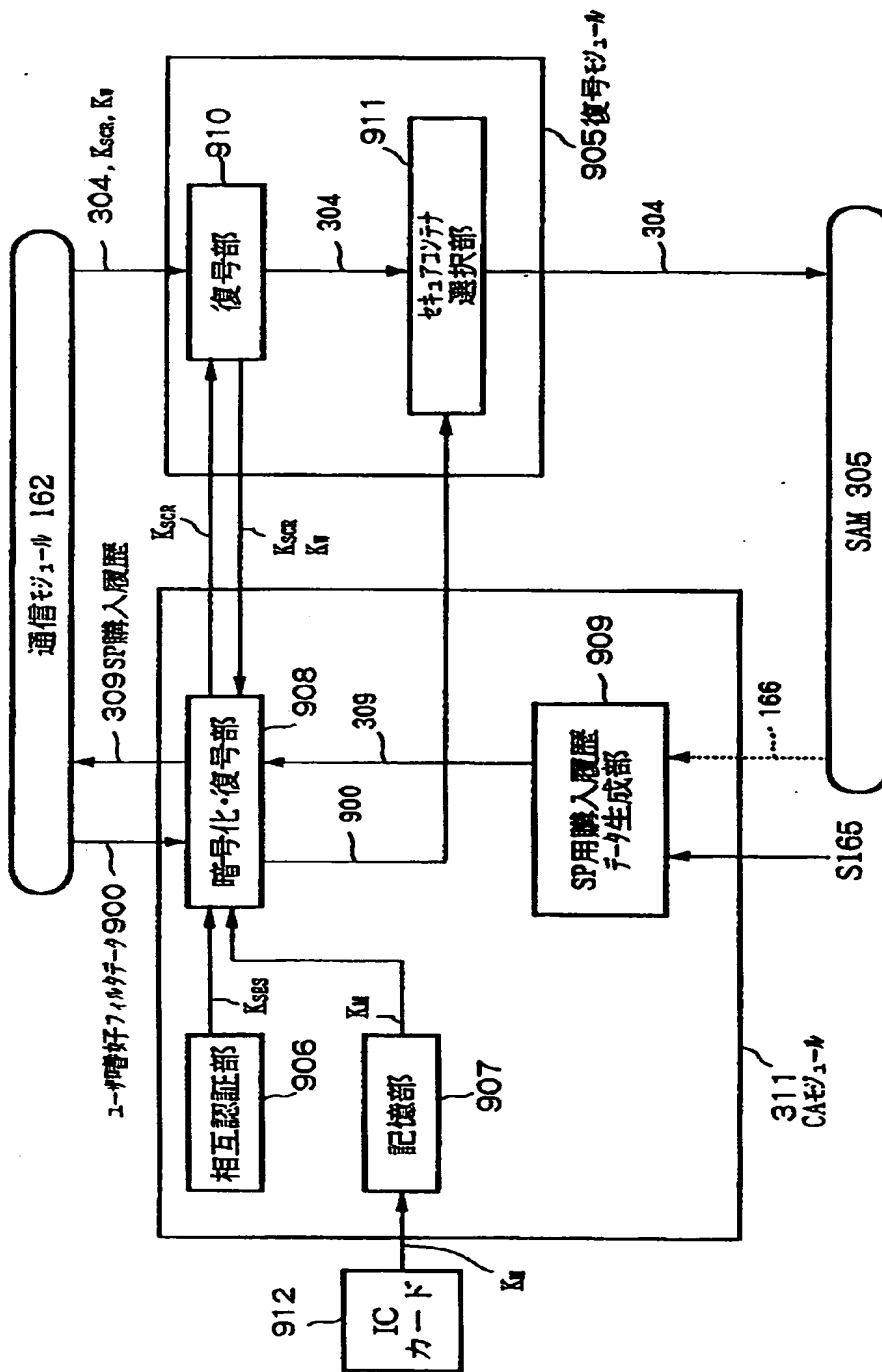
キーファイルKFの生成

利用履歴データ基たは決済処理
(CPとSPとの間の利益分配処理)

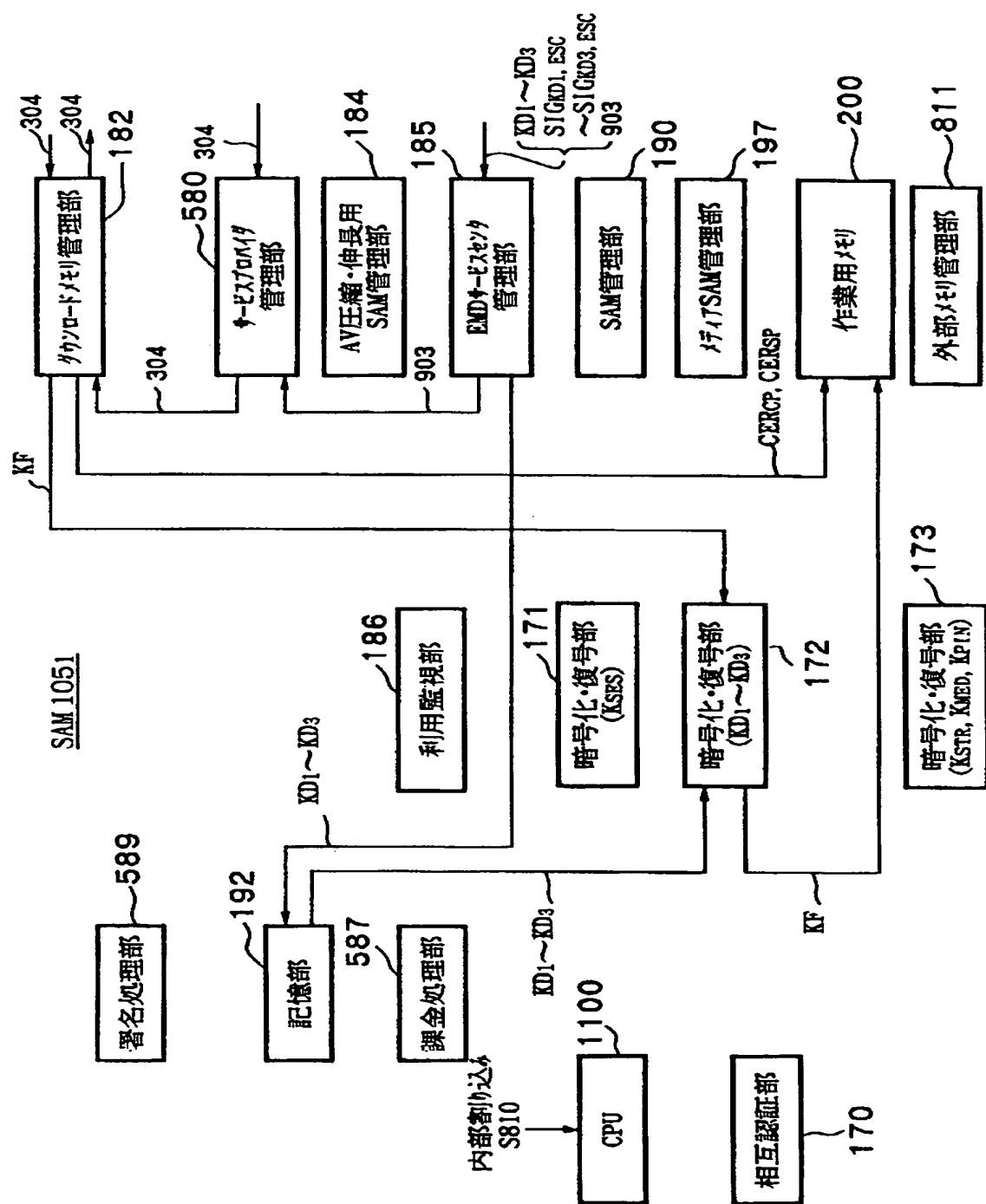
【图 8 8】



【図 8 9】



【图 9 0】



【図 9 1】

作業用メモリ200の記憶データ

コンテンツ鍵データKc

権利書データ(UCP)106

不揮発性メモリ201のロック鍵データK_{Loc}

コンテンツプロバイダ301の公開鍵証明書データCER_{CP}

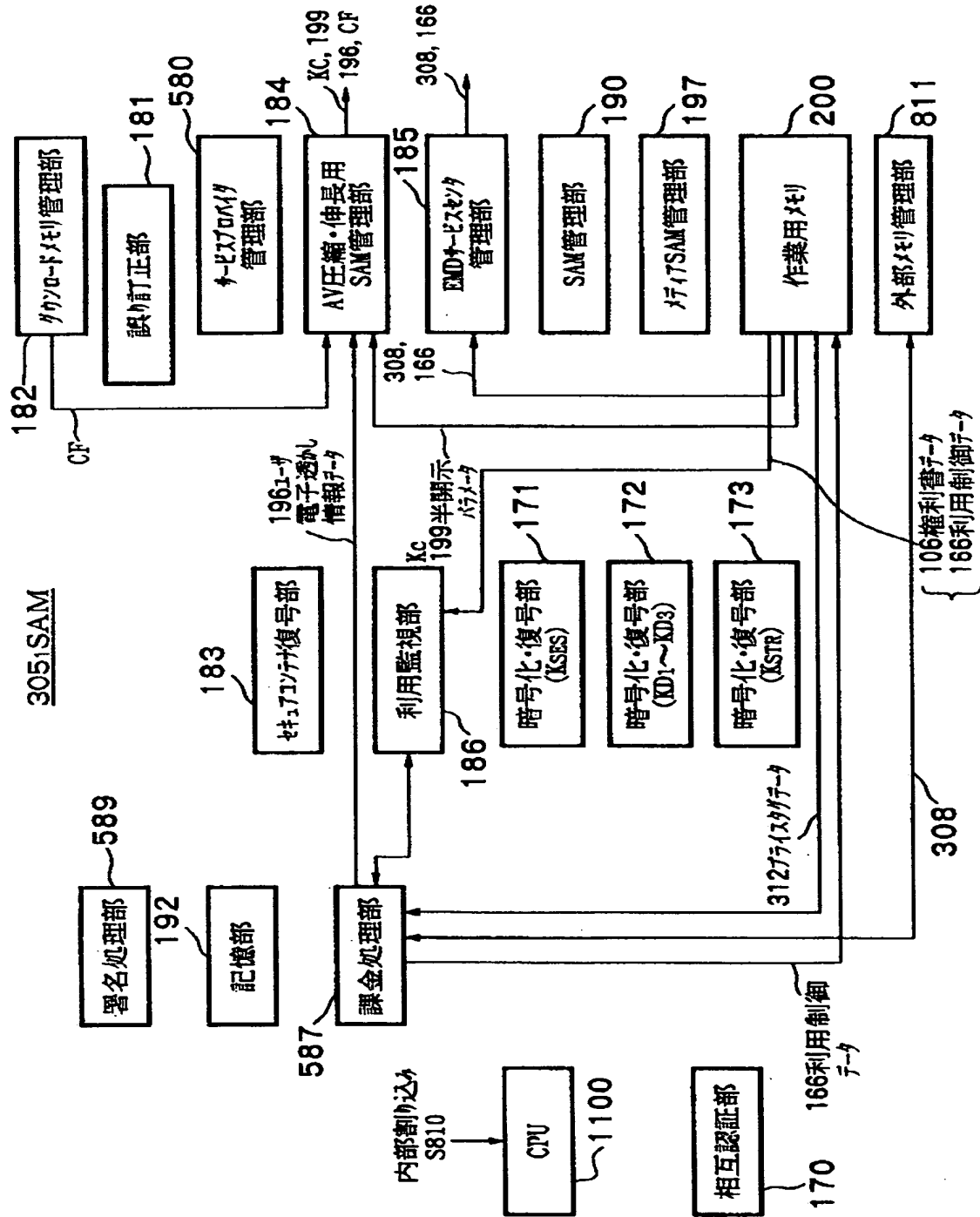
サービスプロバイダ301の公開鍵証明書データCER_{SP}

利用制御データ(UCS)166

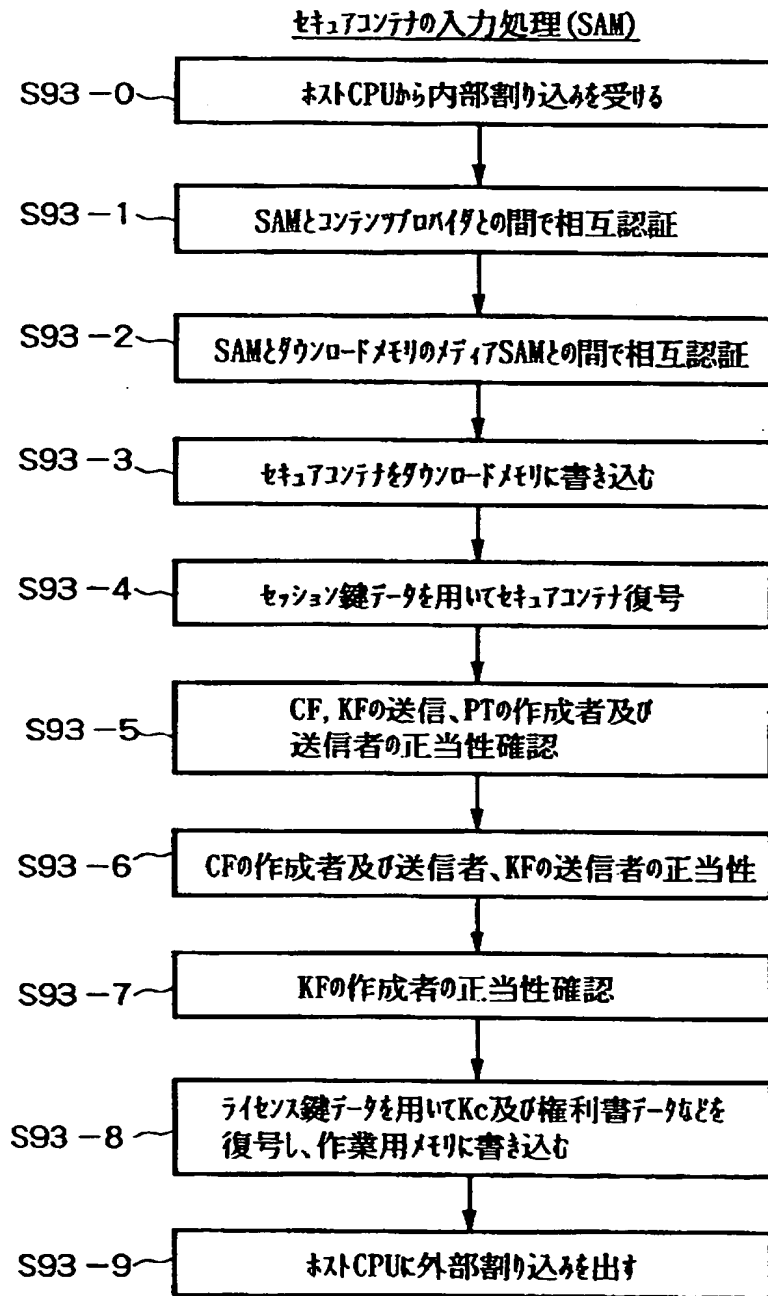
SAMプログラム・ダウンロード・コンテンツSD₁～SD₃

プライスタグデータ312

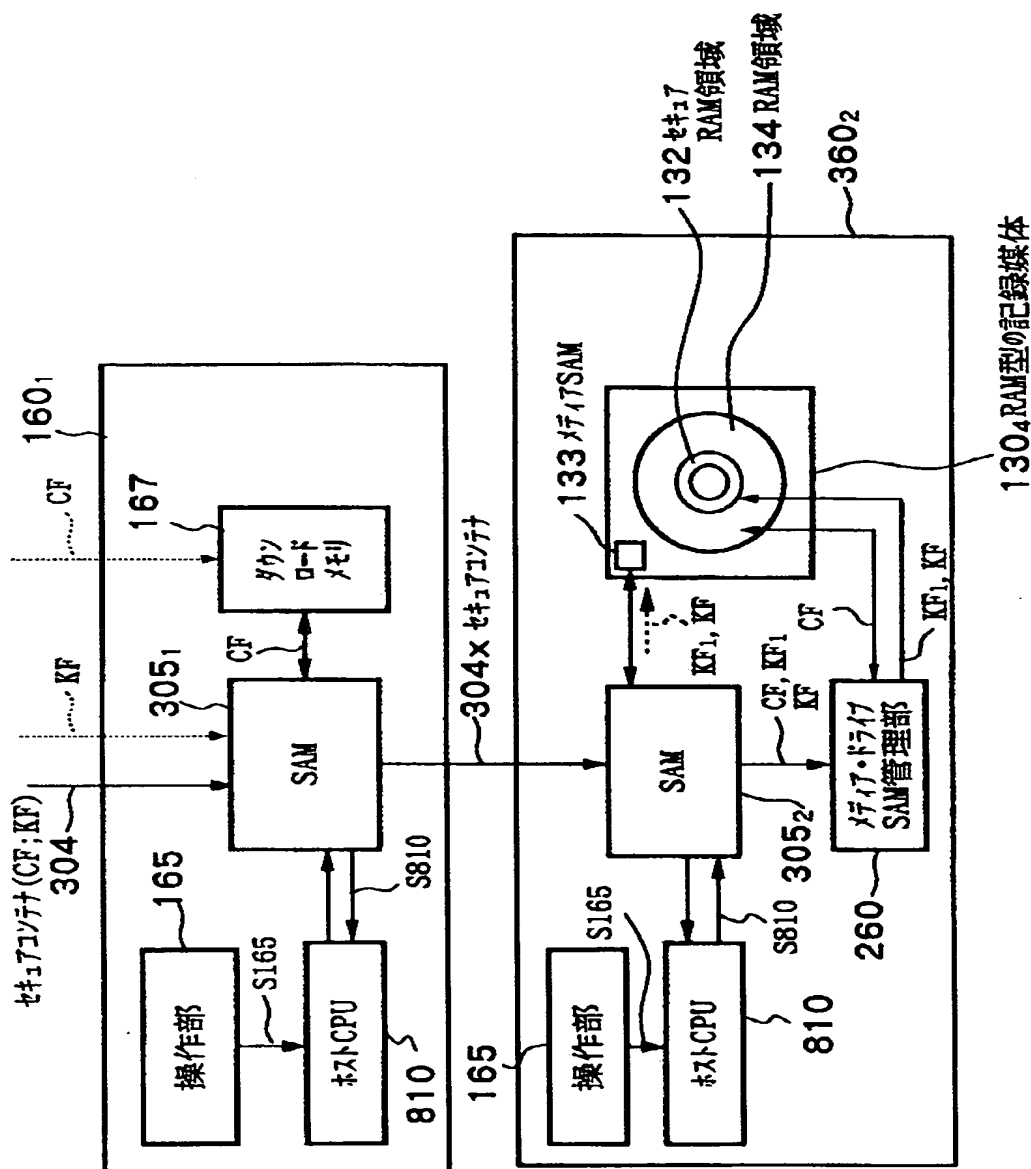
【図 9 2】



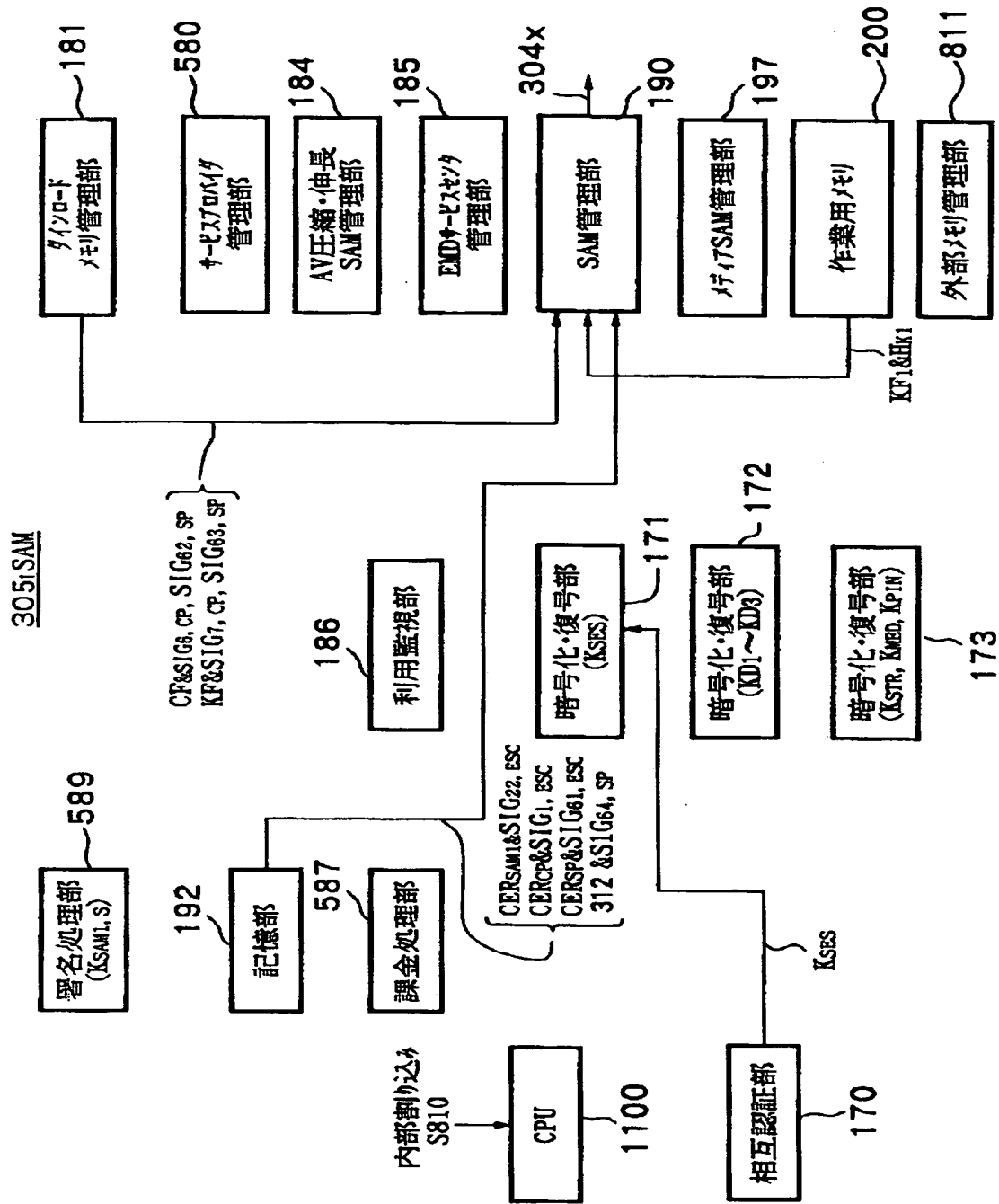
【図 9 3】



【図 9 4】

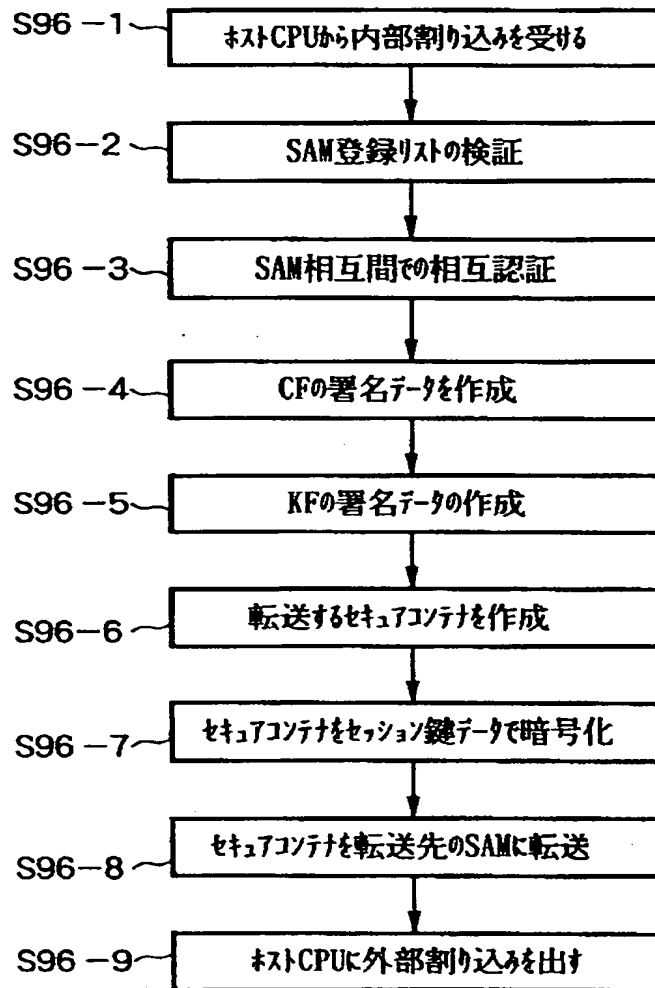


【図 9 5】

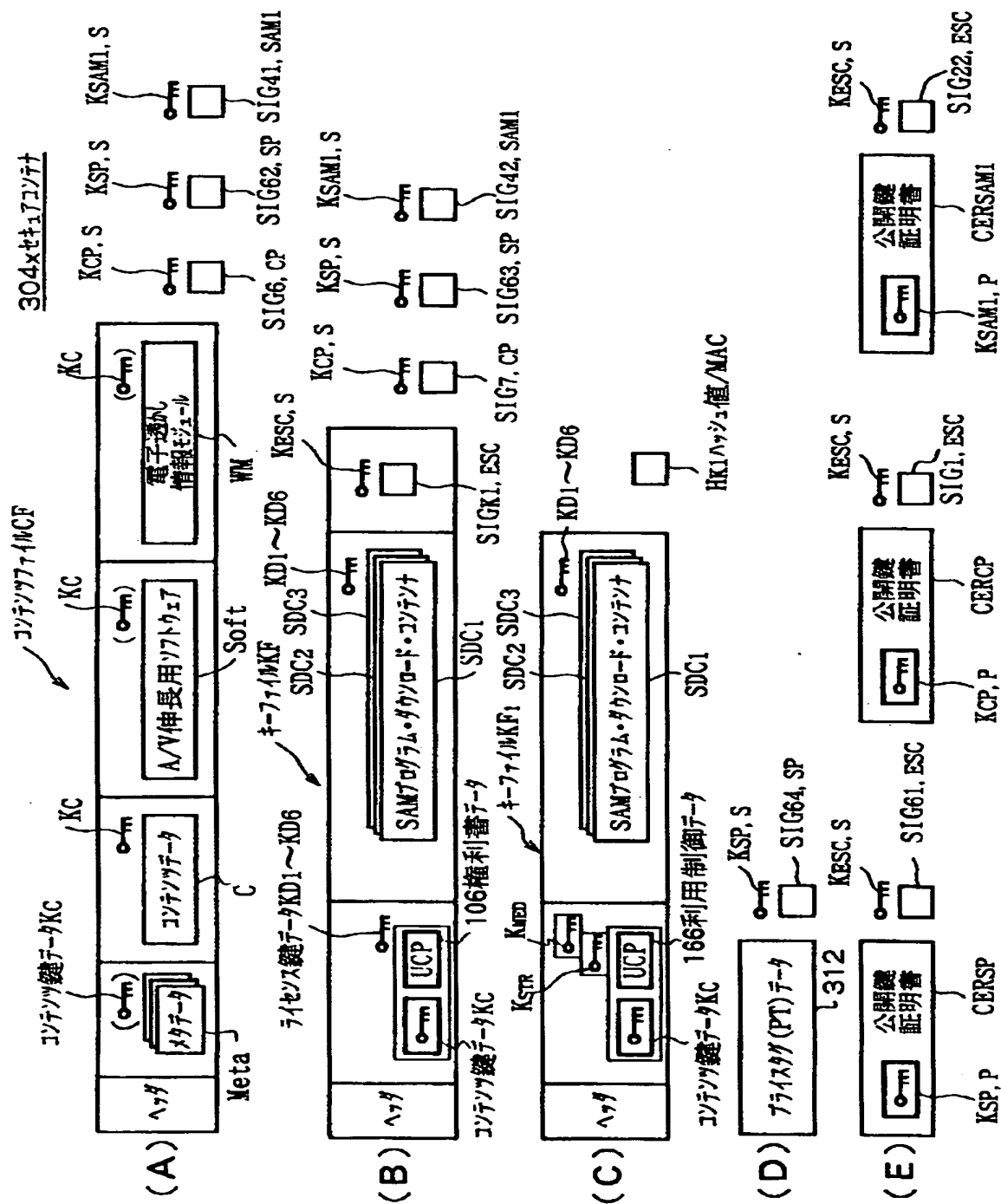


【図 9 6】

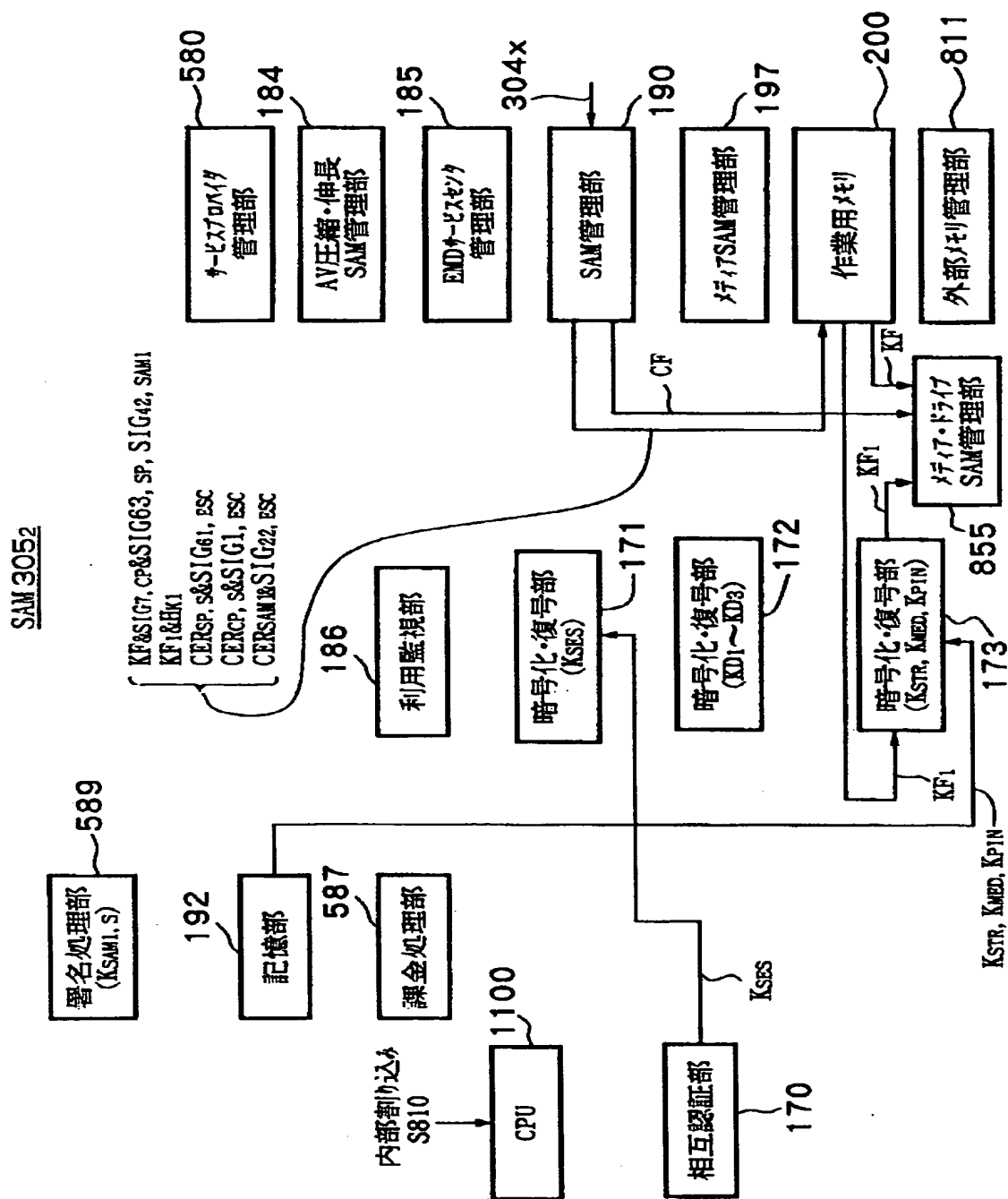
一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送元のSAMの処理 (SAM3051)



【图 9-7】

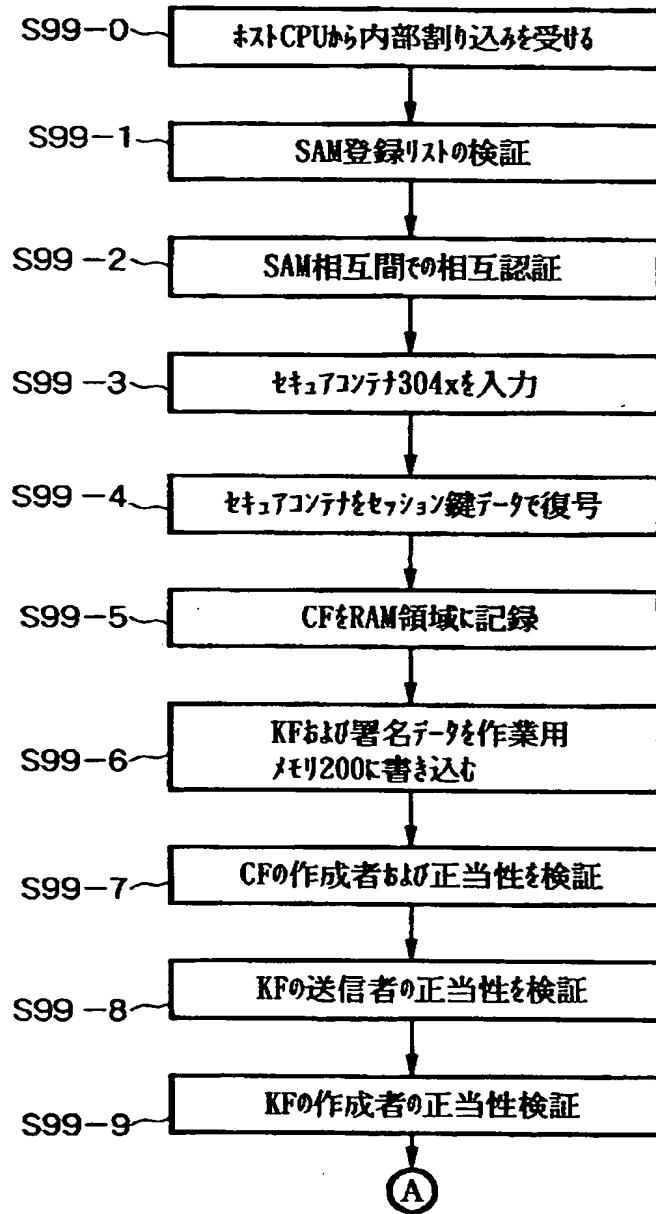


【图 9 8】

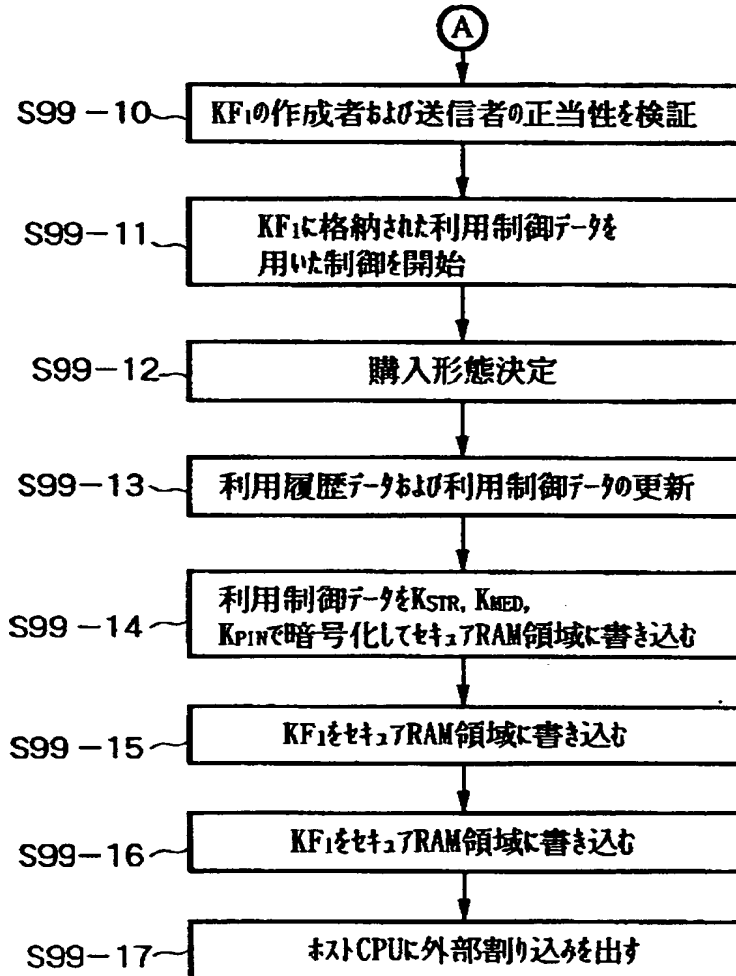


【図 9 9】

一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送先のSAMの処理 (SAM3052)

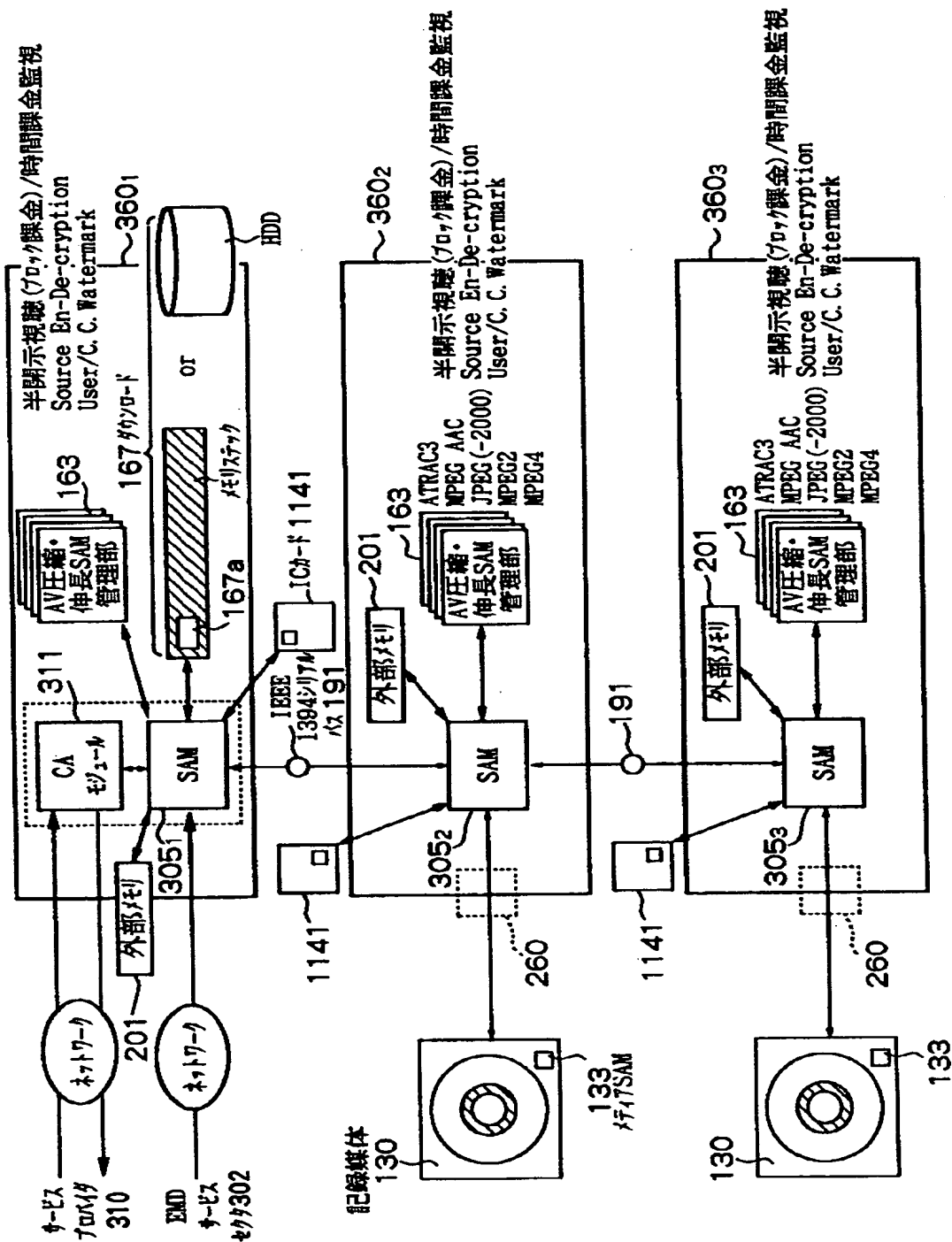


【図 1 0 0】

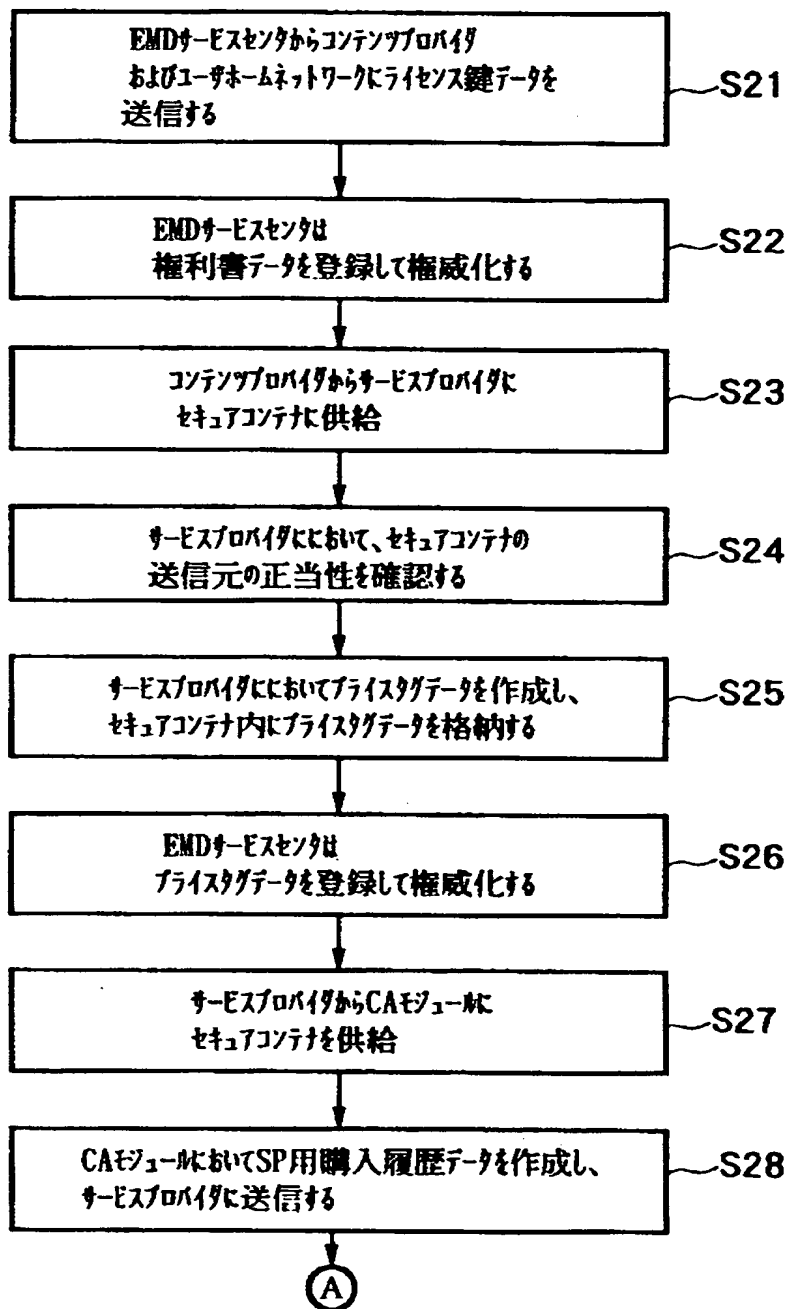


【図 1 0 1】

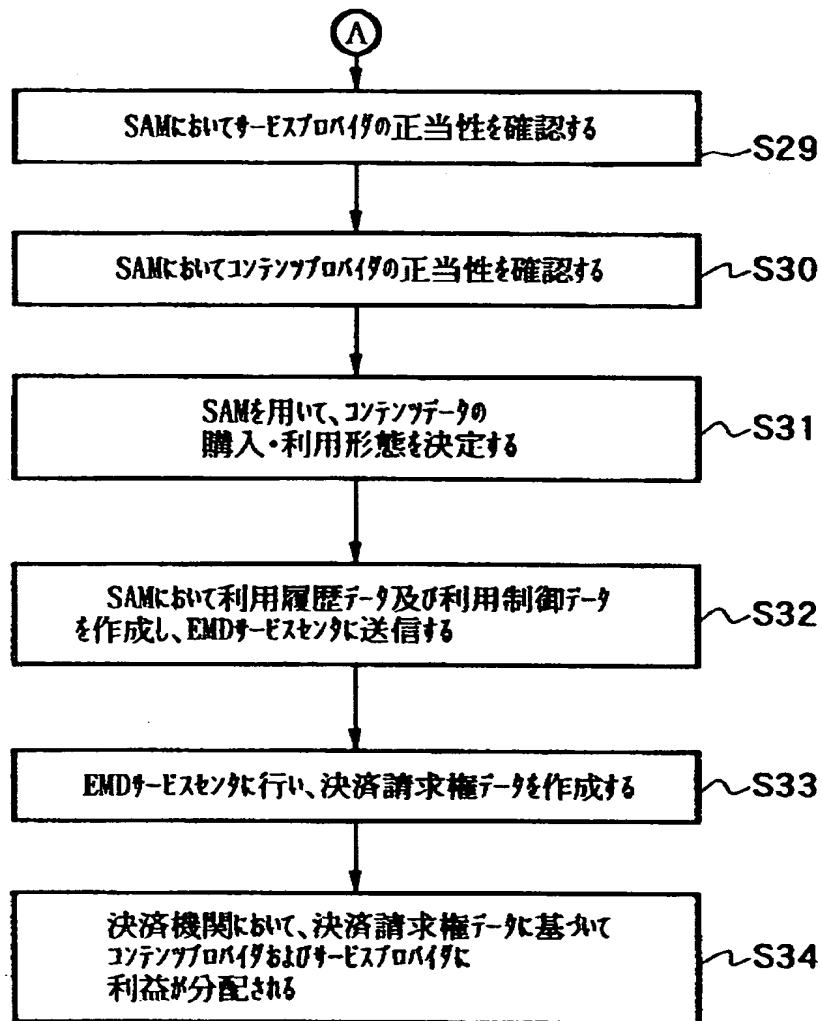
303



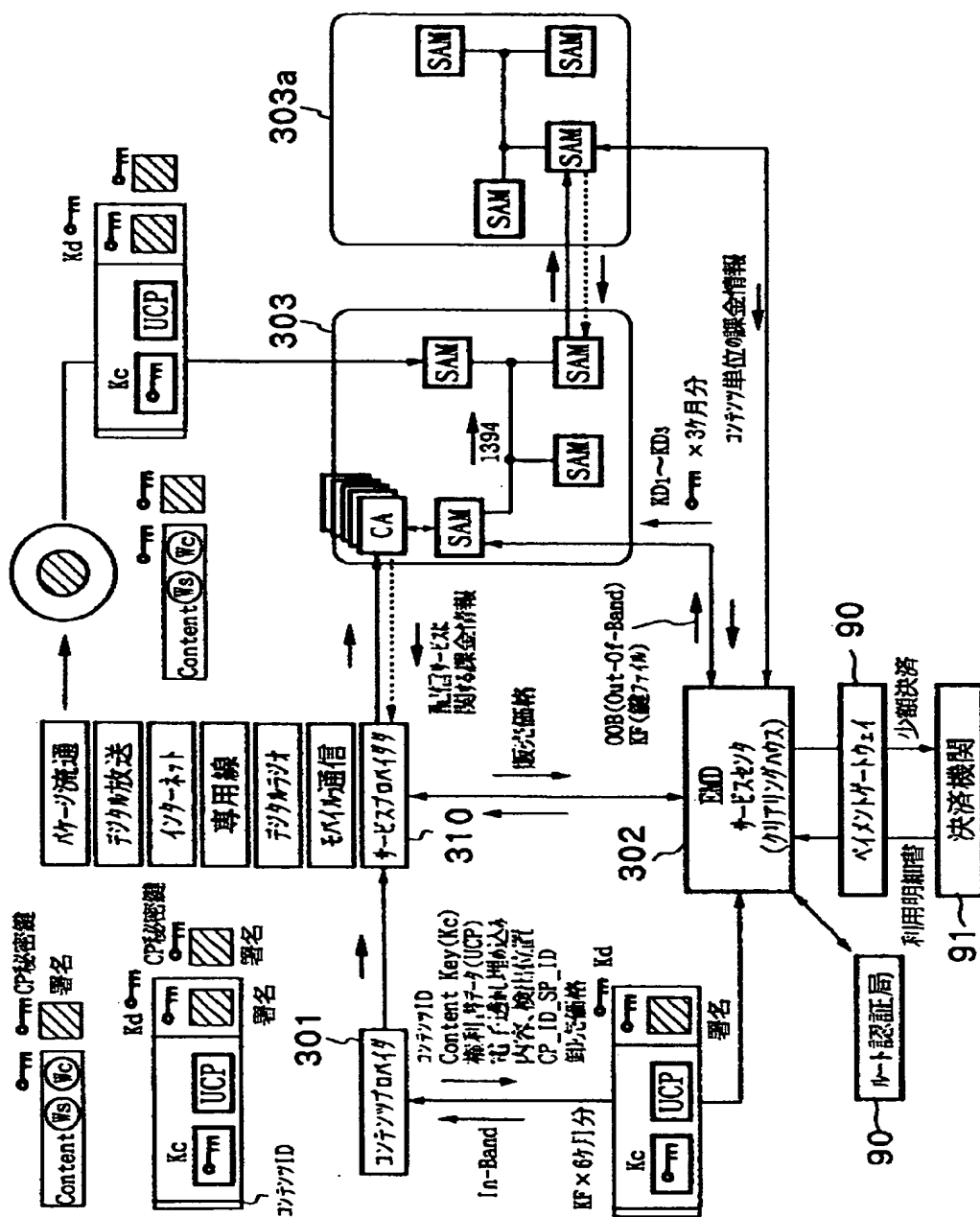
【図 1 0 2】



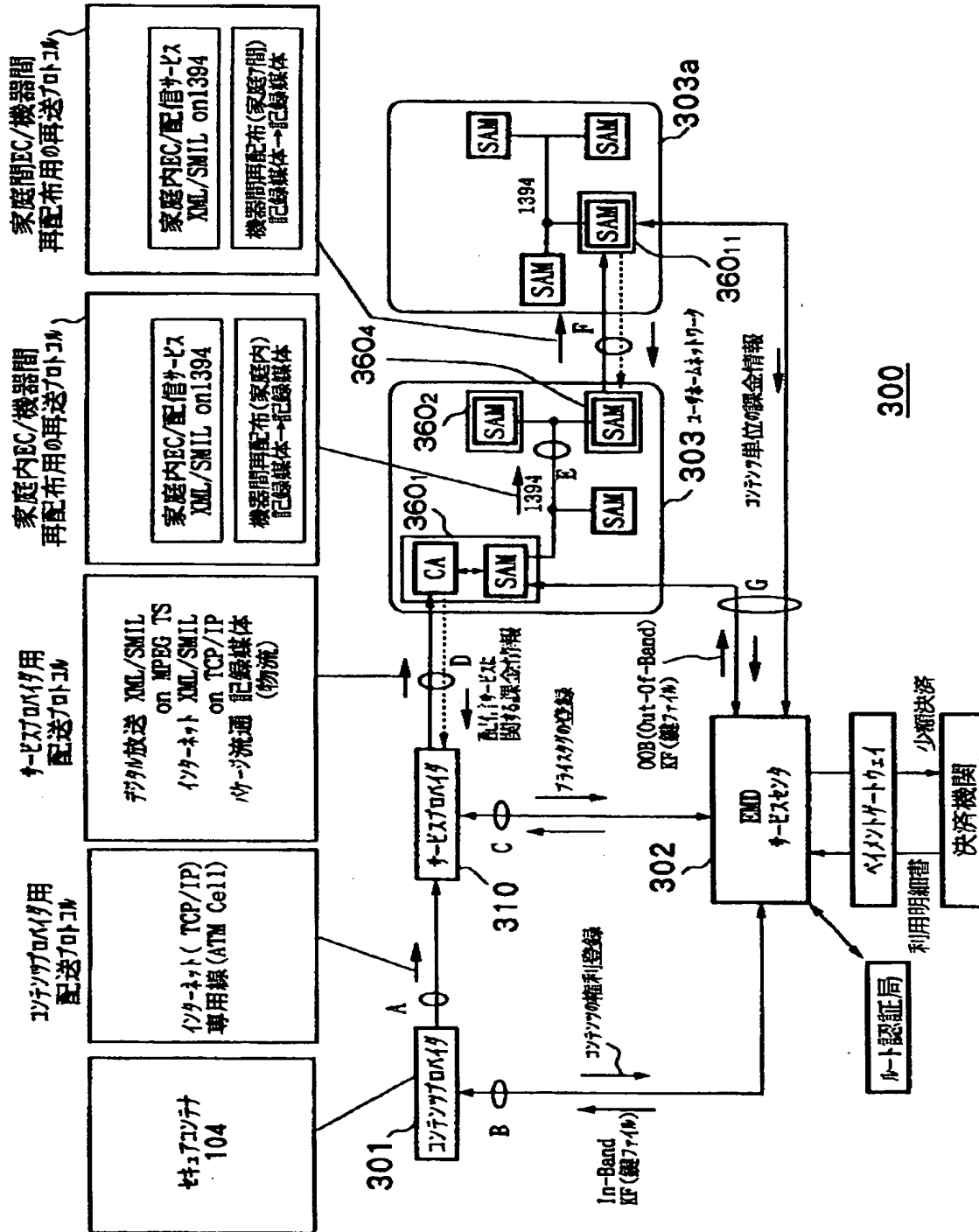
【図 1 0 3】



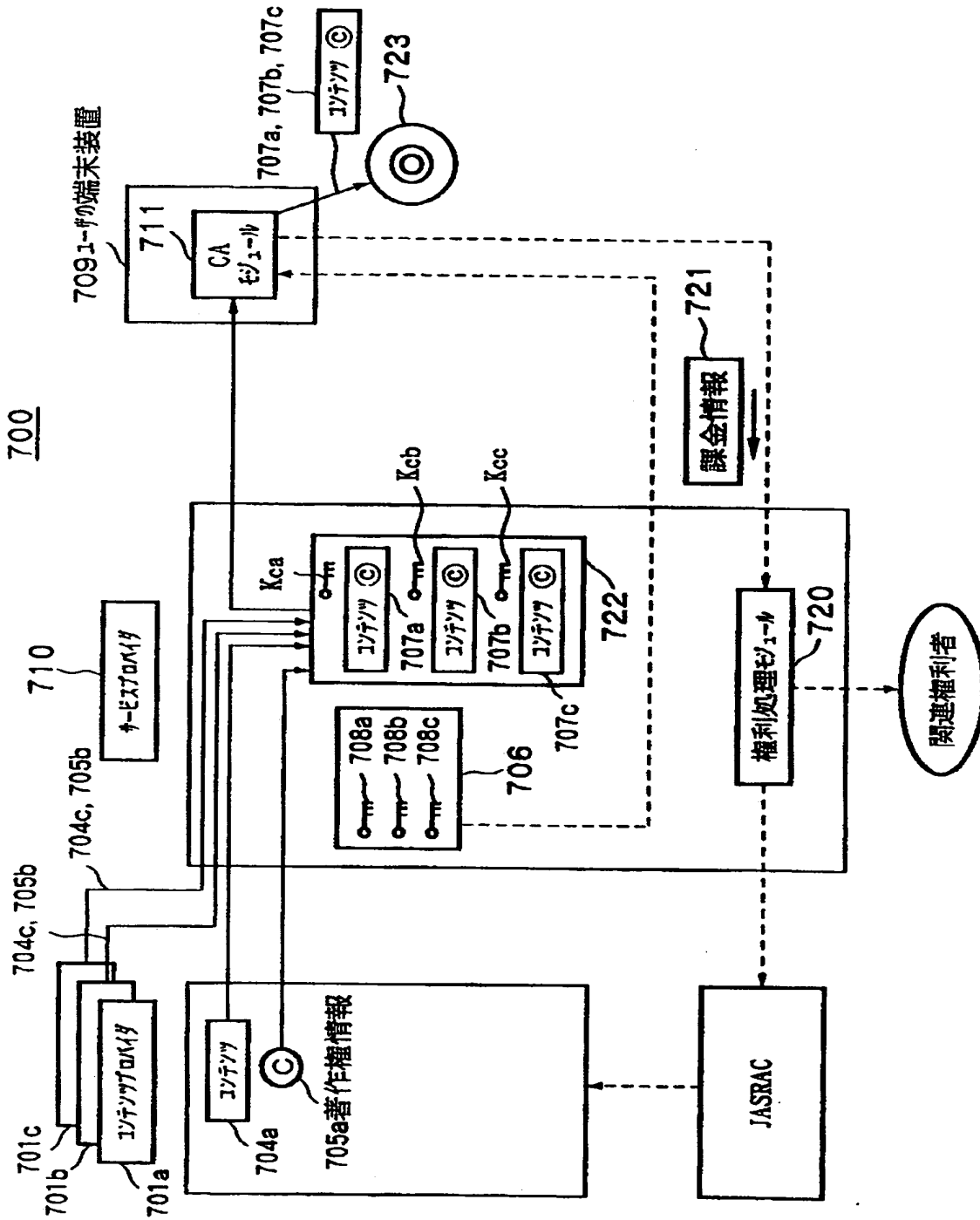
【図 104】



【図 105】



【图 106】



【書類名】 要約書

【要約】

【課題】 コンテンツデータの提供者の利益を効果的に保護できるデータ処理装置を提供する。

【解決手段】 SAM105₁ は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したセキュアコンテナ104を入力し、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。SAM105₁ は、ホストCPU810のスレーブとして機能すると共に、ホストCPU810との共有メモリを有している。

【選択図】 図22

特平 11-361225

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社